ISSA Information Systems Security Association
Colorado Springs Chapter
WWW.ISSA-COS.ORG

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 10 NUMBER 5 MAY 2021

More On Tap for May

Welcome to the month of May! Another month for insightful chapter meetings, mini seminars, and networking. Throughout our region, Cyber-related events are picking up speed and taking off – *and our own chapter is no exception!*

Last month our chapter tore through April with a huge roar. On top of hosting a successful panel discussion focused on unraveling the recent SolarWinds Orion ® breach, we also hosted another session of our monthly mini seminars. Both events where very well attended with positive reviews from the participants. And if that was not enough, we also held our annual 3-day, Cyber Focus Symposium (CFS). This year, CFS was a virtual event produced by Secret Sauce Events (shout out to Dennis O'Neill) and was hosted on the online Whova application; the same application used to host our 2020 Peak Cyber Symposium. As a result, attendance for CFS expanded to over 650 attendees from all four corners of the country – even from as far away as Alaska and Hawaii! We had many phenomenal guest speakers and breakout sessions and the return of our Cleared Careers job fair and Splunk/Epoch Concepts Capture the Flag competition. Like I said, April was a **busy** month!

A Note From Our President

By Mr. Ernest Campos

Looking forward to the month of May, we will enjoy a long-awaited presentation from the Cybersecurity Software Distribution (CSD) company. The CSD company profile many of their corporately developed solutions designed to tackle various Cybersecurity pain points that plague our industry. This will be one presentation you will not want to miss so please register early and invite a co-worker, mentee, or friend to attend as well.

This month ISSA-COS is also providing a huge congratulations to our top five corporate members. These are the companies with the most members in our chapter. We appreciate the strong support these companies and their employees provide to our chapter, our region, and our industry. Would your company like to break into the top five list? If so, contact us and we will tell you how. Not only will your employees reap the

(Continued on page 4)

No Shortage Of Paranoia

By Staff, Strategy Page, April 18, 2021

"Kim Jong Un spent many years in the West getting an education and keeping up to date on new tech, especially computers."

Since the 1990s North Korea has been training more and more Internet software engineers and hackers, even though North Korea has limited access to the Internet. They made the best of their situation by having North Korean Internet engineers build an intranet. This is an Internet type network for North Korea that has no access to the rest of the Internet. By 2010 this intranet program included a locally created own operating system, based on Unix, for North Korean PCs. Called Red Star, it features a front end that makes it look identical to Microsoft Windows. One difference was a custom browser called "My Country" that, for example, can only use a local search engine called "My Country BBS." North Korean computer users can only search the North Korean Internet, with only a few people allowed access to the international Internet. Most of the world wide web users belong to North Korean Cyber War organizations, or Internet security personnel who decide what to import for use on the isolated North Korean Internet.

Details of how this unique North Korea "Internet" and hacker development were scarce until 2015, when South Korea struck an intelligence goldmine when a North Korean colonel defected. This colonel worked for military intelligence, more specifically the RGB (Reconnaissance General Bureau), which runs the hacking operations and espionage operates agents in South Korea and China. The RGB colonel was able to provide details of major changes North Korea hacking operations since 2009. The RGB was formed in 2009 by combining several other intel agencies and that required a lot of data to get reorganized and combined. RGB handles a lot of Cyber War operations and provides information for attacks on South Korea. This includes the 2010 North Korea artillery and torpedo attacks that almost revived the Korean War. South Korea realized that getting an RGB insider was a big deal as it not only provided more details on who is doing what in North Korea, but what exactly is going on between China and North Korea and what role China was playing in the expanding North Korean hacking efforts.

The 2015 defector also made it possible to more quickly detect and analyze new North Korean hacking campaigns. For example, the defector explained how the RGB had different bureaus for the various intelligence specialties. Bureau 121 handled Cyber Warfare research and hacking teams operating in North Korea and China. With the leads provided by the 2015 defector South Korea was better prepared to track North Korea hacking and intelligence operations.

In late 2020 this led to the discovery that North Korean leader Kim Jong Un had created another RGB hacking organization, Bureau 325, that handled special assignments and reported directly to Kim and not the head of the RGB. Before the end of 2020 Kim ordered Bureau 121 transferred to the control of Bureau 325. Kim Jong Un was making hacking operations his own personal project. This was really no surprise because Kim Jong Un's father, the late (since 2011) Kim Jong Il) had always been a big fan of PCs and electronic gadgets in general. While Kim Jong Il ruled he founded Mirim College to train hackers and backed this new school consistently. The only instance of Kim Jong Il's displeasure was suspicions about those who graduated from Mirim between 1986 through the early 1990s. These graduates had been tainted by visits (until 1991) by Russian electronic warfare experts. Some Mirim students also went to Russia to study for a semester or two. All these students were suspected of having become spies for the Russians, and most, if not all, were purged from the Internet hacking program. Thus, it wasn't until the late 1990s that there were a sufficient number of trusted Internet experts that could be used to begin building a Cyber War organization.

Read the rest here:

https://www.strategypage.com/htmw/htiw/articles/20210418.aspx

Membership Corner

Membership Update

Have you updated your contact information on the ISSA International website? You have! That is awesome. If you have not, please log onto the ISSA International website and click on your welcome icon on the top of the page and select "Account + Settings". Once there you can make your updates. Thank you for your support.

We need all members to spread the word that we are looking for new members to join our great organization. Below are the top 10 reasons join ISSA!

Top 10 Reasons Cybersecurity Professionals Join ISSA

1. Build professional relationships
2. Learn practical/best practices solutions
3. Keep up on developments in information security/risk/ privacy
4. Career information and employment opportunities
5. Content of chapter meetings
6. Advance the profession
7. Professional development or educational programming offerings
8. Give back to the profession
9. Earn CPEs/CPUs
10. Develop the next generation of cybersecurity professionals

Our membership is hanging in at ~343 members as of the end of April 2020. Please watch the newsletter, communications and eVites to ensure you stay aware of what's going on in the chapter. As always, if you have any membership questions don't hesitate to contact me or Craig Westerfield, Deputy VP-Membership.

Thanks,

Craig Westerfield

VP-Membership
membership@issa-cos.org

New Members April 2021	
Mitchell R Martinez	Dylan D. Nelson
Dr. Andrew Heo	Robert Hoffman
TaLisa Rickert	Kyler W. Andis
Rio Duckett	Shaun A. Phelps
Cody R. Sheehan	Shannon C. Reinthaler
Jason M. Chambers	

Update Your Profile!

Don't forget to periodically logon to *www.issa.org* and update your personal information.

A Note From Our President

(Continued from page 1)

benefits of membership but, your company will also be appropriately recognized by our chapter. So, without further ado, here are the top five companies in our chapter.

1. L3Harris Technologies
2. Northrop Grumman
3. Booz Allen Hamilton
4. Jacobs Technology
5. SecureSet Academy

In closing, I extend a special thanks to all our board members and key personnel. These are volunteers to work tirelessly to keep the operation of our chapter moving forward. Without their support and dedication, our chapter would not be able to host and present so many fine events throughout the year. If you have a chance, take time to thank a volunteer. They will greatly appreciate your support.

Sincerely,

Ernest

INL RESEARCHERS PUBLISH BOOK TO PREVENT CYBERSECURITY DISRUPTIONS, TRAIN WORKFORCE

Idaho National Laboratory Press Release, February 2, 2021

Two cybersecurity researchers at Idaho National Laboratory have published a new book to help train employees at public utilities to recognize cybersecurity vulnerabilities and develop measures to defend their networks from increasingly sophisticated cyberattacks.

Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering, written by Andy Bochman and Sarah Freeman, details INL's innovative approach to securing critical infrastructure systems like the electric power grid, oil and natural gas refineries and water treatment facilities. Developed in the pre-internet era, much of the technology responsible for controlling operations at many public utilities is often decades-old and lacks modern defense capabilities. This makes them vulnerable to cyberattacks ranging from ransomware threats to significant service disruptions.

To address this challenge, INL developed and pioneered a think-like-the-adversary cybersecurity approach called Consequence-driven Cyber-informed Engineering (CCE). The method acknowledges the fragility of internet-connected technology and services. Instead of relying on traditional protection strategies like intrusion detection software or additional firewalls, INL's cybersecurity approach uses engineering design principles to prevent top tier cyberattackers from damaging or disrupting utilities' most essential operations.

Read the rest here:

https://inl.gov/article/inl-researchers-publish-book-to-prevent-cybersecurity-disruptions-train-workforce/

Instructions & Credit for Online Playbacks of ISSA-COS Training Sessions

- Video playbacks are available to ISSA-COS members within 3-days
- Navigate to the www.issa-cos.org website
- Login using your *COS Chapter* credentials
- Navigate to "Training" and select the desired month
- Select the desired presentation and enjoy the playback
- Upon completion of the playback, email: certification@issa-cos.org and identify the *month* and *session number* for the episode you viewed.

Book Report

By Jay Carson, Security+, CIPP/E, Semper Sec LLC, ISSA-COS Member-at-Large

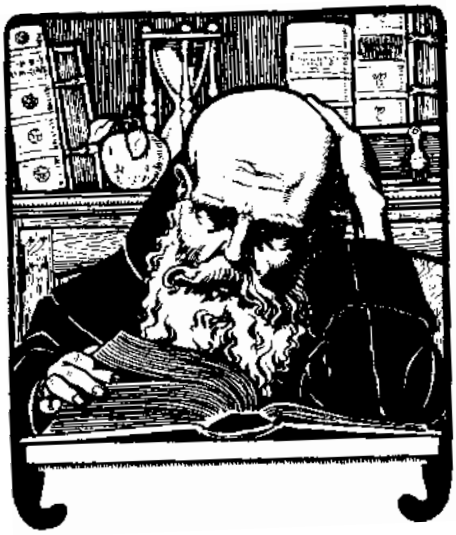
How many important books have you read three times? I am just starting my second of three readings of the cybersecurity and privacy text outlined below. General Eisenhower, so I read someplace, read Clausewitz's *Vom Kreige* (*On War*) three times. I would not place the following book in quite that category. But if you want a single volume textbook, written in a reasonably readable fashion, blending traditional cybersecurity with current privacy management topics, in my opinion this is it!

> Stallings, Dr. William. *Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices.* Addison-Wesley (Pearson Education, Inc.), 2020. I believe it was originally published in 2019.

The author is quite credentialed and experienced, including having an MIT PhD in Computer Science. You should be able to get a paperback copy from one of the online vendors for about $65 including shipping. You would not want to borrow my 471-page copy, as it is too worn from reading! While it is not written like a relaxing mystery story, you can / should read this book cover-to-cover! You regularly do much tougher reading and study, as the certification exam review guidelines often number well over 1,000 pages.

As a privacy professional, I have read a number of privacy management textbooks. There are many out there competing for your cash. Some are good, some are simply a repeating of material you could get for free. This book teaches well cybersecurity, as a means of helping you be able to understand and apply privacy laws and regulations. Consider these topics from the Table of Contents:

- Security and Cryptography Concepts
- Information Privacy Concepts
- Information Privacy Requirements and Guidelines
- Information Privacy Threats and Vulnerabilities
- System Access
- Malicious Software and Intruders
- Privacy in Databases
- Online Privacy
- Other Privacy Enhancing Technology Topics
- Information Privacy Governance and Management
- Risk Management and Privacy Impact Assessment
- Privacy Awareness, Training, and Education
- Event Monitoring, Auditing, and Incident Response
- The EU General Data Protection Regulation
- U.S. Privacy Laws



(The last topic includes as clear a rundown on the California Consumer Privacy Act as I have seen.)

Whether you are in the first years of the profession or are well-experienced and educated in some or most of these topics, I will hazard a guess that this book will help you fill in any gaps!

Happy cybersecurity reading!

The FBI is remotely hacking hundreds of computers to protect them from Hafnium

By Sean Hollister, The Verge, April 13, 2021

In what's believed to be an unprecedented move, the FBI is trying to protect hundreds of computers infected by the Hafnium hack *by hacking them itself*, using the original hackers' own tools (via *TechCrunch*).

The hack, which affected tens of thousands of Microsoft Exchange Server customers around the world and triggered a "whole of government response" from the White House, reportedly left a number of backdoors that could let any number of hackers right into those systems again. Now, the FBI has taken advantage of this by using those same web shells / backdoors to remotely delete themselves, an operation that the agency is calling a success.

"The FBI conducted the removal by issuing a command through the web shell to the server, which was designed to cause the server to delete only the web shell (identified by its unique file path)," explains the US Justice Department.

The wild part here is that owners of these Microsoft Exchange Servers likely aren't yet aware of the FBI's involvement; the Justice Department says it's merely "attempting to provide notice" to owners that they attempted to assist. It's doing all this with the full approval of a Texas court, according to the agency. You can read the unsealed search and seizure warrant and application right here.

It'll be interesting to see if this sets a precedent for future responses to major hacks like Hafnium. While I'm personally undecided, it's easy to argue that the FBI is doing the world a service by removing a threat like this — while Microsoft may have been painfully slow with its initial response, Microsoft Exchange Server customers have also now had well over a month to patch their own servers after several critical alerts. I wonder how many customers will be angry, and how many grateful that the FBI, not some other hacker, took advantage of the open door. We know that critical-but-local government infrastructure often has egregious security practices, most recently resulting in two local drinking water supplies being tampered with.

The FBI says that thousands of systems were patched by their owners before it began its remote Hafnium backdoor removal operation, and that it only removed "removed one early hacking group's remaining web shells which could have been used to maintain and escalate persistent, unauthorized access to U.S. networks."

Read the rest here:

https://www.theverge.com/2021/4/13/22382821/fbi-doj-hafnium-remote-access-removal-hack

Pentagon lit up 175M dormant IP addresses before Trump left office – here's why says new report

By Ryan Morgan, American Military News, April 27, 2021

On Jan. 20, in the final few minutes of President Donald Trump's presidential term, an obscure internet service company announced it was now managing a huge swath of previously unused Pentagon internet protocol (IP) addresses.

The shift in millions of Pentagon IP addresses set off speculation. Following an investigation by the Washington Post revealed on Saturday, a top Department of Defense cybersecurity unit said the effort was meant to determine how malicious internet actors may try to gain control of the Pentagon's IP addresses.

On Saturday, the Washington Post reported that shortly after the Pentagon IP addresses went live, the internet company Global Resource Systems LLC had soon claimed it was managing approximately 56 million of those IP addresses. In the ensuing three months, the Florida-based internet company said the number of Pentagon addresses it manages has risen to nearly 175 million.

Those approximately 175 million IP addresses comprise about six percent of a traditional section of Internet real estate called IPv4. According to the Washington Post, that many IP addresses could sell for billions of dollars on the open market.

Read the rest here:

https://americanmilitarynews.com/2021/04/pentagon-lit-up-175m-dormant-ip-addresses-before-trump-left-office-heres-why-says-new-report/

Understanding the World of Crypto, NFTs, Dapps, DeFi, DEX, and Blockchains

By Shelly Palmer, ShellyPalmer.com, April 25, 2021

Crypto prices and NFTs are hogging the headlines, but they are just the most visible components of a rapidly growing decentralized financial system (DeFi) that has the potential to significantly challenge how we buy, sell, and trade just about everything. Blockchain and cryptocurrency may seem like a new thing, but they have been around for over 10 years. The problem is that the world of crypto can be very confusing with all the jargon, acronyms, and other unfamiliar words. This brief overview will introduce you to some of the basic areas through a series of links to the most prominent organizations, platforms, and toolsets. The full resource page can be found here.

Crypto

Cryptocurrencies (aka "tokens") such as ETH or BTC are created ("mined") when a miner completes a certain amount of computations used to verify transactions that are added to a specific blockchain. (You can learn to mine crypto here.) The miner is rewarded for this effort with a small amount of cryptocurrency. In theory, every ETH or BTC is fungible. Said differently, my 10 BTC or my 50 ETH are worth exactly what your 10 BTC or 50 ETH are worth, and they are interchangeable. There are hundreds of cryptocurrencies that are actively trading on hundreds of exchanges worldwide. Find links to current crypto prices and embeddable price widgets here.

NFTs

NFTs are created ("minted") when a unique, standardized token and associated smart contract are recorded on a blockchain. In theory, NFTs are non-fungible. Said differently, the NFT of Nyan Cat (which sold at auction for $510,945) is unique and not interchangeable with other versions of the same file. Find a list of popular sites where you can mint your own NFTs here.

Crypto Exchanges

Cryptocurrency exchanges act as an intermediary between a buyer and a seller, making money through commissions. You can buy, sell, or trade your crypto for other crypto or fiat currencies. Not all exchanges offer access to all currencies. Choose your exchange carefully to ensure it meets your risk profile, your regulatory requirements, and your trading style. Find a list of the most popular centralized as well as decentralized exchanges (DEX) here.

Decentralization is the key feature of cryptocurrency and its underlying technology. So it might surprise you to learn that most cryptocurrency transactions go through centralized exchanges. Centralized exchanges generally offer a higher degree of reliability and, more importantly, there is a company that you can hold accountable for the execution of your transactions. Most (not all) centralized exchanges must comply with "know your customer" rules and comply with at least some regulatory requirements.

Decentralized cryptocurrency exchanges (DEX) allow users to execute transactions without an intermediary. They are "decentralized." This makes DEX transactions attractive to those who wish to keep their trading activity private. Generally speaking, DEX transactions are crypto-to-crypto. Decentralized exchanges do not facilitate transactions between crypto and fiat currencies.

Digital Wallets

You will need at least one crypto wallet. Do your research. Each wallet has pros and cons, and no single wallet is right for everyone or for every application. There are dozens, if not hundreds, of crypto wallets available. Find a short list of well-established digital wallets here.

Engineering Resources

If you're completely new to distributed ledgers, smart contracts, and crypto and want to write some code, there are many wonderful free resources available online. Here's a list of some excellent smart contract frameworks and other helpful engineering resources.

Dapp and DeFi Assets

Read the rest here:

https://www.shellypalmer.com/2021/04/understanding-the-world-of-crypto-nfts-dapps-defi-dex-and-blockchains/?ck_subscriber_id=1253955602&utm_source=convertkit&utm_medium=email&utm_campaign=Facebook+says%2C+%22Ouch%21%22%20-%205742624

2021 ISSA International Annual Awards Nominations are now OPEN!

Suspense for submissions is 16 May 2021

Every year ISSA International recognizes excellence in information security professionals, the companies they work for, and the chapters to which they belong.

The Colorado Springs Chapter has won numerous ISSA International awards over the years and we hope to continue that amazing trend! Our chapter has two members on the Hall of Fame and six members on the Honor Roll. We've won Chapter of the Year three times, Security Professional of the Year twice, President's Award for Public Service once, and Volunteer of the Year FIVE years in a row!

We need your help in identifying individuals to nominate for the awards described below. If you'd like to recommend someone for any award, please contact the Past Presidents at: past-president@issa-cos.org by the end of March. Additional info about each award can be found on the ISSA International website at: https://www.issa.org/issa-international-awards-2021/?utm_source=WordPress&utm_medium=Organic&utm_campaign=Informz

ISSA International Awards 2021 - ISSA International

Awards Nomination Open on February 15, 2021 (Awards Nomination Now Open). Will close on May 16th, 2021. Hall of Fame is a lifetime achievement award recognizing an individual's exceptional qualities of leadership in their own career and organization as well as an exemplary commitment to the information security profession. Honor Roll is a lifetime achievement

Hall of Fame is a lifetime achievement award recognizing an individual's exceptional qualities of leadership in their own career and organization as well as an exemplary commitment to the information security profession.

Honor Roll is a lifetime achievement award recognizing an individual's sustained contributions to the information security community, the advancement of the association and enhancement of the professionalism of the membership.

The **Security Professional of the Year** honors one (1) individual who best exemplifies the most outstanding standards and achievement in information security in the preceding year.

The **Volunteers of the Year** Award recognizes a member who has made a significant difference to their chapter, the association or the information security community through dedicated and selfless service to ISSA.

The **Organization of the Year** Award recognizes candidates with a sustained, proactive presence that directly contributed to the overall good and professionalism of the association and its membership, providing either services, products and/or direct support that ensures the promotion of the highest ethical standards in addressing information security and its future direction.

Chapter of the Year recognizes chapters that have done an exceptional job of supporting ISSA's mission, serving their member communities and advancing the field. Award are given in small, medium, and large chapter categories.

The password hall of shame (and 10 tips for better password security)

By Josh Fruhlinger, CSO, April 15, 2021

Pop quiz: What has been the most popular — and therefore least secure — password every year since 2013? If you answered “password,” you’d be close. “Qwerty” is another contender for the dubious distinction, but the champion is the most basic, obvious password imaginable: “123456.”

Yes, tons of people still use “123456” as a password, according to NordPass's 200 most common passwords of the year for 2020, which is based on analysis of passwords exposed by data breaches. The six-digit sequence has also ranked high on other lists over the years; SplashData, which has come up with lists using similar methodology, found "123456" in second place in 2011 and 2012; it then jumped up to number one where it stayed every year right through 2019.

Plenty of other epically insecure passwords continue to make the annual password hall of shame, including the aforementioned “password” (always in the top five, and No. 1 in 2011 and 2012); “qwerty” (always in the top ten); and a slightly longer variation of the reigning champ, “12345678” (always in the top six).

10 most common passwords of 2020

These are the 10 most frequently used and worst passwords of 2020, according to NordPass's most common passwords list:

1. 123456
2. 123456789
3. picture1
4. password
5. 12345678
6. 111111
7. 123123
8. 12345
9. 1234567890
10. senha

Other worst password lists, like SplashData's and those from the U.K.’s National Cyber Security Center are mostly consistent. Easily guessed number sequences, and "words" made up of letters immediately adjacent to one another on a standard QWERTY keyboard, are always popular; so is the phrase "iloveyou," because we are a species of hopeless romantics. Another constant cringe-inducing winner is the word "password." On that note, one new addition to NordPass's list this year was "senha," which is Portuguese for — you guessed it — "password." This may reflect Brazil's burgeoning population becoming more connected to the internet, though they're apparently not any more security conscious than English speakers.

Here are the most common passwords for the past three years:

Read the rest here:

https://www.csoonline.com/article/3526408/most-common-passwords.html

To become a guest speaker,
e-mail us at:
SpeakersBureau@issa-cos.org

The 'Sort of" Book Report: Reading ISSA International's Chapter Manual

By Jay Carson, Security+, CIPP/E, Semper Sec LLC, ISSA-COS Member-at-Large

When I started volunteering for our chapter, despite the efforts of two great mentors and multiple supportive colleagues, I felt overwhelmed. I am primarily a learn-by-reading person. I felt I must be missing some information about the inner workings of ISSA chapters generically. Since ISSA has been around over 30 years, they must have the 'things I wanted to know' written down. What about a manual explaining things? Why should I feel I was in new territory, as certainly things with which I was dealing had been experienced before?

Answers: I did not have to be concerned! Things are indeed written down! There is a 136-page manual of recommendations on how to do things, and it is easily available to ISSA members!

To access the manual, just go to the ISSA International website, log in, and go to the 'Chapters' pull down tab. Click on 'Chapter Resources,' and you will see it.

Please do not feel bad if you may not have yet heard about the manual! I attended a recent ISSA International Chapter Leader's Meeting where I learned others have not heard about it. Even the current Chapter of the Year nomination application has an (if applicable) block to check on the chapter manual marked "Did not know it exists." Despite being three years since the last edition (I know, cybersecurity pros consider anything from even last month out-of-date!), the manual is full of reasonable expectations, and useful techniques to achieve those expectations.

While I personally think every board member and all of the key personnel would find it worth their time to read the basic 136-page manual cover-to-cover, it is designed as a reference tool. If your time does not allow that level of study, skimming the manual for situational awareness is also valuable. There are terrific sections on the duties of the chapter treasurer (be appreciative of your chapter treasurer, they have a complicated and very detailed job!), tax status, chapter insurance details, other legal considerations, finding presentation speakers, etc., etc. Also, while I confess I have not yet read them all, there are supplemental documents full of detail and templates on:

- Chapter Organization & Governance
- Membership
- Leadership & Engagement
- Meetings
- Sponsorship & Vendor Relations
- Communications & Marketing
- Awards & Recognition
- Financial Management
- Conferences & Events
- Exhibiting at Conferences or Trade Shows
- Partnering with other Organizations
- Special Interest Groups
- ISSA Education Foundation

An administrative manual is not a page-turning spy story. But if you want to know 'why we do what we do,' this document will help you!

I saved the best for last! ISSA International is sponsoring work in 2021 on a revision to the manual, as well as a chapter playbook! There are plenty of volunteering opportunities for you clear-headed writers!

Happy professional reading!

White House launches plan to protect US critical infrastructure against cyber attacks

By Graham Cluley, TripWire, April 15, 2021

The White House is reportedly moving swiftly forward with a plan to harden the security of the US power grid against hacking attacks.

According to *Bloomberg*, the Biden administration has a plan to dramatically improve how power utilities defend themselves against attacks from countries considered to be adversaries in cyberspace – such as Russia, Iran, North Korea, and China.

The six-page draft plan, drawn up by the National Security Council, is said to provide incentives for electricity companies to safeguard the grid, and hopes to speed up the detection of attempted hacks through monitoring equipment and better synchronise threat intelligence.

Top executives working in the power industry are said to have been briefed privately on the plan last month by US Energy Secretary Jennifer Granholm and Deputy National Security Adviser Anne Neuberger. The hope is that the plan will see the government and industry working more closely together, improving their communication related to cybersecurity issues, and co-ordinating a response when needed.

The power grid is considered the most critical infrastructure to defend from attack, as all other public services depend upon it. But in due course the initiative would be rolled-out to other critical sectors such as refineries, pipelines, and municipal water systems.

Enhancing the ability of utilities to fend off hackers is complex.

For most businesses, the most important thing to maintain is “confidentiality” – keeping data out of unauthorised hands.

When it comes to utilities like the US power grid, however, the overriding concern is “availability” – maintaining a service for the public.

This inevitably can influence decision-making when it comes to cybersecurity. For most organisations, installing a security patch against a software flaw is a no-brainer. But if a computer system is essential for ensuring that a city receives electricity, questions might be reasonably asked as to whether the risk of applying a patch is worth it.

And, of course, asking power providers to beef up their security isn’t going to come cheap – which may mean more expensive energy bills for consumers.

Read the rest here:

https://www.tripwire.com/state-of-security/featured/white-house-plan-protect-critical-infrastructure-against-cyber-attacks/

CISA Releases ICS Advisory on Real-Time Operating System Vulnerabilities

Original release date: April 29, 2021

CISA has released Industrial Control Systems Advisory ICSA-21-119-04 Multiple RTOS to provide notice of multiple vulnerabilities found in real-time operating systems (RTOS) and supporting libraries. Successful exploitation of these vulnerabilities could result in unexpected behavior such as a crash or a remote code injection/execution.

CISA encourages users and administrators to review the ICS Advisory for mitigation recommendations and available updates.

Strategic Partnership

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Comments/Questions: INFO@ISSA-COS.ORG 3

Murray Security Services Sponsorship

- $2,500 per quarter = $10,000 commitment
- 4 **CODERED** Licenses to be provided as give-always at ISSA-COS Events ($1000 value)
- $1000 off (preferred pricing) on most all MSS Professional Training & Certification courses. (no-one else receives this type of standard discount)
- Providing 2 (free) training classes later this summer. Value: $5,000. C|TIA & ESCA

Comments/Questions: INFO@ISSA-COS.ORG 4

MURRAY SECURITY SERVICES
INFORMATION & CYBER SECURITY TRAINING & CONSULTING

EC-Council
Hackers are here. Where are you?

ISSA Colorado Springs Chapter

EC-Council CODERED

CODERED is EC-Council's subscription-based learning platform which allows you to access bite sized content through a clean, simple learning platform!

- **Premium Content:** 4000+ Premium Videos
- **Fresh Content:** New courses and content are added weekly to our library to keep you up-to-date with the latest skills and technologies.
- **Practical Content:** The courses published on **CODERED** contain an abundance of demo lab videos that dive deeper into important cyber concepts and gives you the practical technical knowledge you need to advance your career and improve your performance as a cyber professional.

Comments/Questions: INFO@ISSA-COS.ORG 5

MURRAY SECURITY SERVICES
INFORMATION & CYBER SECURITY TRAINING & CONSULTING

EC-Council
Hackers are here. Where are you?

ISSA Colorado Springs Chapter

Certified Threat Intelligence Analyst (C|TIA)

The Certified Threat Intelligence Analyst (CTIA) program is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe.

The aim is to help organizations hire qualified cyber intelligence trained professionals to identify and mitigate business risks by converting unknown internal and external threats into quantifiable threat entities and stop them in their tracks.

MURRAY SECURITY SERVICES
INFORMATION & CYBER SECURITY TRAINING & CONSULTING

EC-Council
Hackers are here. Where are you?

ISSA Colorado Springs Chapter

EC-Council Certified Security Analyst (ECSA): Penetration Testing

The ECSA penetration testing course provides you with a real-world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available.

It covers the testing of modern infrastructures, operating systems and application environments while teaching the students how to document and write a penetration testing report.

Comments/Questions: INFO@ISSA-COS.ORG 7

ISSA Colorado Springs Chapter

Upcoming Events

Annual Cyber SIG Summit – Jun 18, 2021

- Eight (8) Special Interest Groups (SIGs) profiled
- Half-day event; 1PM – 5PM

Annual Cyber Social – Jun 18, 2021

- No cost to attend; Free to all Community Partners
- ISSA-COS 30th Anniversary Celebration

Comments/Questions: INFO@ISSA-COS.ORG 10

(Continued on page 9

ISSA Information Systems Security Association Colorado Springs Chapter

Social Media

- **Twitter**
  - Colorado Springs ISSA
  - @COSISSA
  - https://twitter.com/COSISSA
- **LinkedIn**
  - ISSA Colorado Springs Chapter
  - https://www.linkedin.com/groups/1878203/
  - https://www.linkedin.com/in/issa-cos-7495361b2
- **Facebook**
  - Colorado Springs Chapter of the ISSA
  - @ColoradoSpringsISSA
  - https://www.facebook.com/ColoradoSpringsISSA
- **Instagram**
  - issa_cosprings
  - https://www.Instagram.com/issa_cosprings/




Comments/Questions: INFO@ISSA-COS.ORG

ISSA Information Systems Security Association Colorado Springs Chapter www.issa-cos.org

ISSA-COS SALUTES ALL OUR CURRENT **COMMUNITY PARTNERS!**

THANK YOU FOR ALL YOU DO TO SUPPORT OUR CHAPTER AND OUR COMMUNITY!

TOGETHER WE ARE STRONGER

WWW.ISSA-COS.ORG

NSA-CISA-FBI Joint Advisory on Russian SVR Targeting U.S. and Allied Networks

Original release date: April 15, 2021

CISA, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) have released a Joint Cybersecurity Advisory (CSA) on Russian Foreign Intelligence Service (SVR) actors scanning for and exploiting vulnerabilities to compromise U.S. and allied networks, including national security and government-related systems.

Specifically, SVR actors are targeting and exploiting the following vulnerabilities:

CVE-2018-13379 Fortinet FortiGate VPN
CVE-2019-9670 Synacor Zimbra Collaboration Suite
CVE-2019-11510 Pulse Secure Pulse Connect Secure VPN
CVE-2019-19781 Citrix Application Delivery Controller and Gateway
CVE-2020-4006 VMware Workspace ONE Access

Additionally the White House has released a statement formally attributing this activity and the SolarWinds supply chain compromise to SVR actors. CISA has updated the following products to reflect this attribution:

Alert AA20-352A: APT Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
Alert AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments
Malware Analysis Report AR21-039A: MAR-10318845-1.v1 - SUNBURST
Malware Analysis Report AR21-039B: MAR-10320115-1.v1 - TEARDROP
Table: SolarWinds and Active Directory/M365 Compromise - Detecting APT Activity from Known TTPs
Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise web page

CISA strongly encourages users and administrators to review Joint CSA: Russian SVR Targets U.S. and Allied Networks for SVR tactics, techniques, and procedures, as well as mitigation strategies.

CISA and NIST Release New Interagency Resource: Defending Against Software Supply Chain Attacks

Original release date: April 26, 2021

A software supply chain attack—such as the recent SolarWinds Orion attack—occurs when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers. The compromised software can then further compromise customer data or systems.

To help software vendors and customers defend against these attacks, CISA and the National Institute for Standards and Technology (NIST) have released Defending Against Software Supply Chain Attacks. This new interagency resource provides an overview of software supply chain risks and recommendations. The publication also provides guidance on using NIST's Cyber Supply Chain Risk Management (C-SCRM) framework and the Secure Software Development Framework (SSDF) to identify, assess, and mitigate risks.

CISA encourages users and administrators to review Defending Against Software Supply Chain Attacks and implement its recommendations.

ISSA-COS Sponsorship Plans

ISSA-COS Annual Financial Sponsorship Packages	Platinum	Gold	Silver	Bronze	Single Event
	$19,995	$14,995	$9,995	$4,995	$2,495
Name/Logo recognition in the following channels					
a. Chapter website	X	X	X	X	X
b. Mass-marketing emails	X	X	X	X	X
c. Monthly newsletter	X	X	X	X	X
d. On-screen recognition at scheduled events	X	X	X	X	X
Preferred Guest Speaker for the following events					
a. Cybersecurity Special Events	X	X	X	X	X
b. Chapter Meetings and Mini Seminars	X	X	X		
c. Cyber Focus Symposium	X	X			
d. Peak Cyber Symposium	X				
Discounted Exhibitor Packages for conferences					
a. Cyber Focus Symposium: 5' x 8' (Full Price: $1,495)	-$500	-$400	-$300	-$200	-$100
b. Peak Cyber Symposium: 5' x 8' (Full Price: $1,495)	-$500	-$400	-$300	-$200	-$100

Material Sponsors		
Type	Qty	Fee
Training Vouchers	12	$12,000
Shirts	250	$4,000
Padfolios	250	$2,200
Lapel Pins	250	$800
Book Bags	250	$400
Notepads	250	$200
Pens	250	$150
Stickers	250	$100
Logo Socks	250	$2,500
Logo Beanies	250	$3,000
Sponsor's Choice	250	TBD
Venue/Facility	n/a	$0

Comments/Questions: SPONSORSHIPS@ISSA-COS.ORG 1

Mentorship

Executives of U.S. technology companies told lawmakers on February 23 that a recent breach of corporate and government networks was so sophisticated that a nation had to be behind it and said all the evidence points to Russia.

Read the rest here:

https://www.rferl.org/a/russia-hack-computer-technology-us-government/31118886.html

Mentorship is a relationship between two people, a mentor, and a mentee. A mentor is an experienced and knowledgeable individual who passes their knowledge and experience to a mentee so they may gain a solid footing into their chosen career field. This relationship is an extremely valuable tool for both the mentor and the mentee.

For the mentee, it provides invaluable insight into building a successful career by which the mentor helps the mentee establish measurable short- and long-term goals that are attainable and relevant for their chosen information system security career field. For the mentor, it provides an opportunity to lead and develop our future generation of information system security specialists. This partnering relationship is essential for providing knowledge, advice, motivation, and encouragement for successful mentee development and positive information system security career field growth.

Did you know that ISSA-COS has a mentorship program? Well, it is true! ISSA-COS has a mentorship program and we are looking for mentors that are wanting to contribute to developing our future generation of information system security specialists. We are also looking for a mentorship committee chair to lead our mentorship program. If you are interested in volunteering to be a mentor or are interested in leading our ISSA Mentorship Committee, please contact memberservices@issa-cos.org.

Steven Mulig
ISSA-COS, VP-Membership

Craig Westerfield
ISSA-COS, Deputy VP-Membership

MENTORING PROGRAM

The ISSA-COS Mentoring Program provides a connection between individuals (mentees) seeking career guidance, industry information, or personal encouragement with individuals (mentors) who have an aptitude for sharing their career experiences, industry resources, and personal talents for the benefit of the mentee. Mentees derive from every conceivable background and exist at every stage of professional development. Mentoring sessions are designed to ensure the confidentiality, integrity, and availability of information shared between the participants.

To help facilitate the mentoring process, ISSA-COS has adopted the S.M.A.R.T. goal setting model to safeguard a consistent development process that is equally understood and honored by mentees and mentors alike. As such, the Mentoring Program supports the following objectives of ISSA-COS:

For more information about mentoring, email: *mentorship@issa-cos.org*

- Promote increased professional education opportunities for members
- Provide career guidance and professional development approaches
- Encourage balance between technical skillsets and soft skills such as time management, task management, workplace conduct, and business savvy
- Increase member knowledge of available resources designed to strengthen skillsets
- Encouraging an open exchange of Cybersecurity related techniques, approaches, and problem-solving skills
- Promote member education and awareness of Cybersecurity security issues and recommended strategies to combat the issues
- Providing opportunities for mentees and mentors to network with other professionals and share their lessons learned from their individual mentoring experiences.

Cyber Spotlight – PARTY!!

ISSA-COS is turning 30 in 2021!

Initiative to document ISSA-COS Chapter History

Interviews with past/current **Presidents**

Interviews with past/current **Board Members**

Interviews with past/current **General Members**

Interviews with **Community Partners**

WWW.ISSA-COS.ORG

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.

Article for the Newsletter?

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

Send your article ideas to the Newsletter at:

newsletter@issa-cos.org

Chapter Officers:

President*: Ernest Campos
Vice President*: Michael Crandall
Executive Vice President*: Scott Frisch
Treasurer: Dennis Schorn
- Deputy: Kurt Danis

Recorder/Historian: Andrea Heinz
- Deputy: **Vacant**

Dir. of Professional Outreach: Katie Martin
- Deputy: Pat Pendergest

Director of Communications : Christine Mack
- Deputy: **Vacant**

Director of Certifications: Derick Lopez
- Deputy: Luke Walcher

Vice President of Membership: Steven Mulig
- Deputy: Craig Westerfield

Vice President of Training: Phebe Swope
- Deputy: **Vacant**

Member at Large 1: Art Cooper
Member at Large 2: Jim Blake
Member at Large 3: James Asimah
Member at Large 4: Jay Carson

Committee Chairs:

Annual Audit: Chris Edmondson
Training: **Vacant**
Mentorship Committee Chair: **Vacant**
Newsletter: Don Creamer
IT Committee: Patrick Sheehan
Speaker's Bureau: Kelli Blanchard
Girl Scouts Cyber Badge Camp: Anna Parrish
Annual Election: Colleen Murphy

**** Executive Board Members***

Past Senior Leadership

Past President: Fred P. Henninge, Jr.
Past President: Russ Dewey
Past President: Mike O'Neill
President Emeritus: Dr. George J. Proeller
President Emeritus: Mark Spencer
Past President: Pat Laverty
Past President: Cindy Thornburg
Past President: Frank Gearhart
Past President: Colleen Murphy

Twitter bug sees users BANNED if they tweet 'Memphis' after the word is mistakenly flagged by the app's automated systems

By Jonathan Chadwick, Daily Mail, March 15, 2021

In one of the weirder social media glitches, Twitter users have been having their account suspended after simply tweeting the word 'Memphis'.

Anyone who tweeted the name of the US city on Sunday received a message telling them they 'violated Twitter's rules against posting private information'.

Offending users could still browse Twitter, but couldn't post tweets, like or retweet other tweets, or follow other users for 12 hours.

Read the rest here:

https://www.dailymail.co.uk/sciencetech/article-9363073/Twitter-users-banned-tweet-word-Memphis-weird-glitch.html