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

ISSA-COS NEWSLETTER

VOLUME 10 NUMBER 6 JUNE 2021

Colorado Springs, Colorado

Kicking Off June

As we kick off the month of June, it is hard to believe the year is nearly half over. Winter is officially behind us (not withstanding an occasional freak snowstorm) and consistently warmer weather is upon us. Yes, the birds are chirping, the flowers are blooming, and the rabbits are rabbiting – *as usual*. If you have not yet prepped your 5th wheelers, travel trailers or RVs then, you'd best get to it!!

As for our chapter, we too are busy, busy, busy. In the month of May, held our monthly Chapter Meeting and Mini Seminar. Our chapter meeting featured the leadership team from Cyber Software Distributors (CSD – http://www.cybersoftwaredistributors.com/). The guest speakers included **Mr. Alfred Ortiz, Mr. William Lenzini,** and **Mr. James Lacey** who collectively spoke to us about "*Endpoint Security: ZeroTrust Infrastructures, Trust but Verify.*" For our Saturday Mini Seminar, **Mr. Chad Eckles** provided a presentation on "*Threat Modeling: Deconstructed*" followed by a technical, hands-on presentation from our own VP of Training, **Ms. Phebe Swope**. We appreciate the presentations provided by all our guest speakers and thank them for sharing their time, knowledge, and experience.

A Note From Our President

By Mr. Ernest Campos

In June, our schedule is stacked with great events. Kicking off the month is the **Virtual CISSP Review**. During this six-session event, participants will review the knowledge domains associated with the CISSP certification in preparation to sit for the exam. To all those who register for this event, we wish you the best of luck and look forward to adding you to the family of CISSP certificate holders.

Later in June, our chapter will host the inaugural Cyber SIG Summit (SIG = Special Interest Group). At this event, we will host virtual presentations for all eight of our SIGs. These groups include the following:

Affinity Groups

- Cyber Women SIG
- Cyber Educator SIG
- Cyber Student SIG
- Cyber CISO SIG

(Continued on page 4)

'World's leading bank robbers': North Korea's hacker army

By Sunghee Hwang, Yahoo News, May 25, 2021

Nuclear-armed North Korea is advancing on the front lines of cyberwarfare, analysts say, stealing billions of dollars and presenting a clearer and more present danger than its banned weapons programmes.

Pyongyang is under multiple international sanctions over its atomic bomb and ballistic missile programmes, which have seen rapid progress under North Korean leader Kim Jong Un.

But while the world's diplomatic focus has been on its nuclear ambitions, the North has been quietly and steadily building up its cyber capabilities, and analysts say its army of thousands of well-trained hackers are proving to be just as dangerous.

"North Korea's nuclear and military programmes are long-term threats, but its cyber threats are immediate, realistic threats," said Oh Il-seok, a researcher at the Institute for National Security Strategy in Seoul.

"Cryptocurrency is attractive because it is uncontrolled, borderless, and relatively anonymous."

Pyongyang's cyberwarfare abilities first came to global prominence in 2014 when it was accused of hacking into Sony Pictures Entertainment as revenge for "The Interview", a satirical film that mocked leader Kim.

The attack resulted in the posting of several unreleased movies online as well as a vast trove of confidential documents.

Since then the North has been blamed for a number of high-profile cyberattacks, including a $81 million heist from the Bangladesh Central Bank as well as the 2017 WannaCry global ransomware attack, which infected some 300,000 computers in 150 nations.

Pyongyang has denied any involvement, describing US allegations over WannaCry as "absurd" and a foreign ministry spokesman declaring: "We have nothing to do with cyberattacks."

But the US Justice Department in February indicted three North Koreans on charges of "participating in a wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks".

In its 2021 Annual Threat Assessment Report, Washington acknowledged that Pyongyang "probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks" across the United States.

The North's cyber programme "poses a growing espionage, theft, and attack threat," said the document from the Office of the Director of National Intelligence.

It accused Pyongyang of stealing hundreds of millions of dollars from financial institutions and cryptocurrency exchanges, "probably to fund government priorities, such as its nuclear and missile programs".

'The best defence'

North Korea's cyber-programme dates back to at least the mid-1990s, when then-leader Kim Jong Il reportedly said "all wars in future years will be computer wars".

Today Pyongyang's 6,000-strong cyberwarfare unit, known as Bureau 121, operates from several countries including Belarus, China, India, Malaysia and Russia, according to a US military report published in July 2020.

Scott Jarkoff of cybersecurity firm CrowdStrike rates them highly: "They are extremely sophisticated, dedicated, and capable of conducting advanced attacks."

Bureau 121 recruits are trained in different coding languages and operating systems at special establishments such as Mirim University, said former student Jang Se-yul, who defected in 2007.

Now known as the University of Automation, it takes in only 100 students a year from among the North's highest-scoring schoolchildren.

"We were taught that we had to be prepared against America's cyberwarfare capabilities," Jang told AFP.

"Ultimately, we were taught that we had to develop our own hacking programmes since attacking the enemy's operating system is the best defence."

Read the rest here:

https://news.yahoo.com/worlds-leading-bank-robbers-north-023011739.html

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 ~346 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,

Steven Mulig

VP-Membership
membership@issa-cos.org

New Members May 2021	
Blaise Contino	Daniel J. Galaska
Robert Drone	James Wacaster
Edward O. Nester	

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)

Industry Groups

Cyber Retail SIG
Cyber Healthcare SIG
Cyber Finance SIG
Cyber DoD SIG

Options for in-person and virtual participation are available. Please register early and invite a friend. This event is open to the public.

Immediately following the Cyber SIG Summit, ISSA-COS will host our first ever Community Cyber Social at **JMark Services** (8415 Explorer Drive, COS, CO 80920). During the social, ISSA-COS will celebrate our 30th Anniversary as a chapter. To celebrate this monumental milestone, ISSA-COS will provide free food, drink, music, and fun as we all take time to unwind, kick-back, and enjoy the evening. ISSA-COS members and community professionals are invited. Representatives from various Cyber-related organizations will be on hand to share information about their own upcoming events. Take time to network with regional professionals and learn what is trending in the industry these days.

In conclusion, ISSA-COS is rabbiting. **We thank you** for all your support and encourage you to continue supporting our organization. The best to do this is to invite a co-worker, friend, or family member to attend an upcoming event. We are always willing to welcome a new face and showcase the benefits of becoming a member of our chapter. To all our existing members, I raise a glass in honor of all you do in your jobs and throughout our community. We appreciate you and your membership with our chapter. *Happy 30th Anniversary!*

Sincerely,

Ernest

OFFICE OF THE PRESIDENT OF ISSA-COS

May 18, 2021

Friends of ISSA-COS,

Recently, the Colorado Springs Chapter of the Information Systems Security Association (ISSA-COS) identified anomalous activities associated with the email account belonging to our Director of Communications. Fortunately, our director quickly recognized the odd activities and immediately notified our IT Committee. Our IT Committee shifted into Incident Response mode and conducted a swift and thorough investigation while isolating the affected email account before further harm could be performed.

Later, the incident investigation revealed ISSA-COS had sustained an external breach against the affected email account. It was also determined a subset of internal and external email addresses were exposed along with an undisclosed number of historical emails. The actor(s) of this attack are now using the gathered information to send phishing attacks to the individuals for whom the stolen email addresses belong. We are not sure how long these phishing attacks will persist. The characteristics of these phishing emails include the following:

- A spoofed email name implying the sender is "**(Communication&issa-cos org)**". Note the "&" and space between "cos" and "org" are not characteristics of our chapter domain name
- A sender address not associated with ISSA-COS; "(**Communication&issa-cos org**) <***sender address***>"
- Poorly written English and a salutation that may or may not include the recipient's name
- A hyperlink to a non-chapter related ZIP file - the contents of which may include malicious files.

ISSA-COS is encouraging anyone who receives an email communication from "**(Communication&issa-cos org) <*sender address*>**" to immediately purge the email from their account. **NOTE HOWEVER**: email communications received from "**Communications@issa-cos.org**" are legitimate and can be trusted.

Other than a subset of personal, public, or professional email addresses, no other Personally Identifiable Information (PII) has been found to be compromised. Since ISSA-COS is a public non-profit organization, we do not store, process, or transmit proprietary information and most of our operational information is publicly available information. This makes us and the information we store of moderately-low to low value outside our organization.

On our end, we have taken the following steps:

- We have reported the incident to our email service provider
- We have isolated and remediated the affected email account
- We have instituted a required password reset on all chapter email accounts
- We have made efforts to contact known recipients of the compromised email addresses
- We have reported the incident to the Chief of Operations (COO) of ISSA International

We are reviewing the security applications, processes, and procedures in place within our organization.

On behalf of ISSA-COS, I apologize for the incident and vow to institute stronger measures to protect our members and our community at large. We encourage you to use this incident as a reason to review, update, and socialize the security practices in place within your own businesses and organizations. Remember, none of us are entirely safe from Cybersecurity attacks but, with a little effort we can be safer. For additional information or questions, please contact us at info@issa-cos.org.

Sincerely,

Ernest M. Campos
President, ISSA-COS

Book Review No. 4—Landoll on Policies

By Jay Carson, ISSA-COS, Member-at-Large, May 31, 2021

You Do Not Have To Read This Book Review Article!

However, we only get one of our own ISSA-COS policy writing experts (you long-time ISSA-COS members know the individual!) to present occasionally. He speaks on writing cybersecurity policies and procedures once a year or so at chapter meetings. You might miss ***our*** guy's talks, both informative and humorous, so read on!

Landoll, Douglas J. *Information Security Policies, Procedures, and Standards: A Practitioner's Reference.* Boca Raton, FL: CRC Press, 2016.

This was only published in paperback in 2020. You can get it by ordering online for under $45. It is only 230 pages. While it has a bit of passive voice, and the subject matter is not gripping like a pen tester's "there I was…." story, it is well worth your time. Yes, it is a slower read, but that does not mean the material presented is not important. In fact, anything that gets a cheapskate like me to pay over $50 to get another of his books must be good:

Landoll, Douglas J. *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, 2nd Edition.* Boca Raton, FL: CRC Press, 2020.

I have it on order and will tell you about it next month.

Douglas J. Landoll is an ISSA member, and a Distinguished Fellow no less! His other credentials include a computer science degree and MBA, plus CISSP and CISA credentials, and 25 years' experience in this profession. So, he certainly should know what he is talking about, and I think he does! You can also find him on LinkedIn.

Because I always try to tell you what is in the book, here is the core of the Table of Contents:

- Information Security Policy Basics

  (Policies, Standards, Guidelines, Baselines, Procedures)
- Information Security Policy Framework

  (Federal Information Security Management Act (NIST 800-53), ISO 27001, COBIT, etc.)
- Information Security Policy Details

  (Exceptions, Levels, etc.)
- Information Security Procedures and Standards
- Information Security Policy Projects

  (Scoping, Roles, Phases, Revisions, Applications)
- Appendices on Example Policies

  (FISMA NIST 800-53) Framework and Example Departmental Policy Tailoring Guide)

So, while as I said you do not have to read this article, I highly recommend you read this book!

As an added benefit, your ability to say you have thoroughly read such an authoritative source should enhance your credibility in any cybersecurity policy discussion.

Happy professional reading!

Book Review No. 5—Kevin Mitnick's Latest Book

By Jay Carson, ISSA-COS, Member-at-Large, May 31, 2021

I hope I do not lose friends and professional mentors by writing this book review. Some of us have very strong negative feelings about Mr. Mitnick, regarding his cyber-criminal past activities. While I do not regard him as heroic, I do regard his writings as well worth your professional reading time. Here goes:

Mitnick, Kevin with Robert Vamosi. *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to be Safe in the Age of Big Brother and Big Data.* New York: Little, Brown and Company, 2017 (2019 edition).

In late May 2021 I attended an online presentation by Mr. Mitnick, and he referenced the book, as containing still-valid information. You can get it by ordering online for under $15. It is 298 pages.

I pay close attention whenever we get a penetration tester as an ISSA-COS presenter, both to the presentation itself and to my fellow audience members. Based on what I see, penetration testing, both the acts and the defenses against hacking, are popular with our membership. Some of you want to become pen testers yourselves. If so since Mr. Mitnick is now a pen tester, I recommend you read this book. Much of what he writes is supported by our past presenters on this subject. Privacy and Open Source Intelligence professionals will also find this book quite useful, as he shows how easy it is to find data to support social engineering offensive actions. Do not worry, as the title states the focus is on defensive actions! Mitnick has some great commentary on passwords, some of which I have not seen or heard elsewhere. Candidly, this is a great book to read before you talk to non-cybersecurity professionals about good cyber hygiene. Probably the most relevant to me was his comments regarding when you think you are secure, but you really are not, as the hacker just has to add in a few more steps!

In order to see if I really wanted to risk writing this book review, I also started reading:

Mitnick, Kevin with William L. Simon. *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker.* New York: Back Bay Books, 2011.

I am well into the book now. This is Mitnick's autobiography. It details how he got into hacking and is helping me understand some of the hacker mindsets. I am forming the opinion some hacking becomes a compulsion, like gambling. The thrill of 'breaking in' became like a drug addiction to him.

He has two other books out there:

Mitnick, Kevin D. and William L. Simon. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers.* New York: Wiley, 2005.

Mitnick, Kevin D. and William L. Simon. *The Art of Deception: Controlling the Human Element of Security.* New York: Wiley, 2003.

I will get back to you on these books.

Happy professional reading!

Cyber Spotlight – PARTY!!

ISSA-COS is turning 30 in 2021!

Friday, June 18, 2021, 5 PM until 8 PM

at Jmark Services, Inc.
8415 Explorer Drive, Suite 110
Colorado Springs

This is how long hackers will hide in your network before deploying ransomware or being spotted

By Liam Tung, ZDNet, May 19, 2021

Cyberattackers on average have 11 days after breaching a target network before they're being detected, according to UK security firm Sophos – and often when they are spotted it's because they've deployed ransomware.

As Sophos researchers note in a new report, that's more than enough time for an attacker to get a thorough overview of what a target network looks like, where its weaknesses lie, and for ransomware attackers to wreck it.

Sophos' data, based on its responses to customer incidents, suggests a much shorter "dwell time" for attackers than data from FireEye's incident response team, Mandiant. Mandiant recently reported the median time-to-detection was 24 days, which was an improvement on previous years.

Sophos explains the relatively short dwell time in its incident response data is because a whopping 81% of incidents it helped customers with involved ransomware – a noisy attack that immediately triggers alarms for tech departments. So while shorter dwell times might indicate an improvement in so-called security posture, it might also be just because file-encrypting ransomware is a disruptive attack compared to data theft.

"To put this in context, 11 days potentially provide attackers with approximately 264 hours for malicious activity, such as lateral movement, reconnaissance, credential dumping, data exfiltration, and more. Considering that some of these activities can take just minutes or a few hours to implement, 11 days provide attackers with plenty of time to do damage," notes Sophos in its Active Adversary Playbook 2021 report.

The vast majority of incidents Sophos responded to were ransomware attacks, suggesting the scale of the problem. Other attacks include stealing data, cryptominers, banking trojans, data wipers, and the use of penetration testing tools like Cobalt Strike.

Read the rest here:

https://www.zdnet.com/article/this-is-how-long-hackers-will-spend-in-your-network-before-deploying-ransomware-or-being-spotted/?&web_view=true

Apple's Security Compromises in China Outlined in New Report

By Juli Clover, MacRumors, May 17, 2021

Apple has been making concessions on privacy and security in order to continue building and selling its devices in China, according to an in-depth report from *The New York Times*.

The focal point of the report is Apple's decision to comply with a 2016 law that requires all personal information and data collected in China to be kept in China, which has led Apple to build a China data center and relocate Chinese customers' iCloud data to China, managed by a Chinese company.

Apple fought against China's efforts to gain more control over customer data, but given China's leverage over Apple, Apple had no choice but to comply. There were initially disagreements over the digital keys that can unlock iCloud encryption. Apple wanted to keep them in the United States, while Chinese officials wanted them in China.

Ultimately, the encryption keys ended up in China, a decision that "surprised" two unnamed Apple executives who worked on the negotiations and who said that the decision could potentially endanger customer data. There is no evidence that the Chinese government has access to the data, but security experts have said that China could demand data or simply take it without asking Apple, especially given compromises in encryption key storage and the fact that a third-party company manages customer data on Apple's behalf.

"The Chinese are serial iPhone breakers," said Ross J. Anderson, a University of Cambridge cybersecurity researcher who reviewed the documents. "I'm convinced that they will have the ability to break into the servers."

In a statement, Apple told *The New York Times* that it "never compromised" the security of users or user data in China "or anywhere we operate." Apple says that it still controls the keys that protect the data of Chinese customers, and the China data center is using the most advanced encryption technology available, which is more advanced than what Apple uses in other countries.

Apple has also been removing apps from the App Store in China at the request of the Chinese government after China began requiring an official license to release an app. Apple told *The New York Times* that it has done so to comply with Chinese laws.

Read the rest here:

https://www.macrumors.com/2021/05/17/apple-security-compromises-china-icloud/

Apple's Find My network can be abused to leak secrets to the outside world via passing devices

By Thomas Claburn, The Register, May 12, 2021

Apple's Find My network, used to locate iOS and macOS devices – and more recently AirTags and other kit – also turns out to be a potential espionage tool.

In short, it's possible to use passing Apple devices to sneak out portions of information from one place to another, such as a computer on the other side of the world, over the air without any other network connectivity.

Fabian Bräunlein, co-founder of Positive Security, devised a way to send a limited amount of arbitrary data to Apple's iCloud servers from devices without an internet connection using Bluetooth Low Energy (BLE) broadcasts and a microcontroller programmed to function as a modem. That data can then be retrieved from the cloud by a Mac application. In a blog post on Wednesday, he dubbed his proof-of-concept service Send My.

Apple's Find My network, when enabled in Apple devices, functions as a crowdsourced location-tracking system. Participating devices broadcast over BLE to other nearby attentive Apple devices, which in turn relay data back over their network connection to Cupertino's servers. Authorized device owners can then get location reports on enrolled hardware through the company's iCloud-based Find My iPhone or iOS/macOS Find My app.

Read the rest here:

https://www.theregister.com/2021/05/12/apples_find_network/?&web_view=true

NIST Seeks Input on HIPAA Security Rule Guidance Update

By Marianne Kolbasuk McGee, GovInfoSecurity, May 4, 2021

The National Institute of Standards and Technology is seeking public comment as it plans to update its 2008 guidance for implementing the HIPAA Security Rule, which went into effect about 20 years ago.

Meanwhile, regulatory experts are debating whether the rule itself needs an update.

NIST is accepting comments through June 15 on updates designed to provide education about information security terms used in the HIPAA Security Rule, amplify awareness of relevant cybersecurity guidance from NIST and others and illustrate how to implement the rule in the current environment.

"Recognizing that covered entities and business associates have diverse ways of implementing the HIPAA Security Rule, NIST is soliciting feedback about how organizations are implementing the [current] resource guide, its application and its use in practice," NIST says.

"NIST's cybersecurity resources have evolved since SP 800-66, Revision 1 ... and stakeholders will benefit from guidance that includes references to these updated resources," the agency notes.

Once comments have been reviewed, NIST will release a draft of its updated HIPAA Security Rule guidance and will again solicit comments before finalizing the document.

Information Sought

NIST is asking covered entities and business associates to describe how their organizations:

- Manage compliance and security simultaneously - for example, complying with the HIPAA Security Rule while also improving cybersecurity posture;
- Assess risk to electronic protected health information - and how this assessment leads to the identification of appropriate security controls and practices;
- Determine that security measures implemented in accordance with the security rule are effective in protecting ePHI and how often they initiate a process to determine effectiveness;
- Manage concerns, including ePHI disclosures, regarding business associates' compliance with the security rule;
- Facilitate internal and external communication about security rule implementation and compliance.

NIST is also asking organizations if they implement "recognized security practices" and how they document the process of demonstrating adequate implementation. Plus, it's asking them to describe how these recognized security practices overlap with and diverge from compliance with the HIPAA Security Rule.

NIST notes that legislation signed into law in January allows the Department of Health and Human Services "to reduce fines and penalties for violations of certain federal privacy standards for health information if an entity subject to those standards has adopted particular cybersecurity practices." (See: *The Final HIPAA Actions Under Trump Administration*).

Time for a Rule Update?

Some security experts are debating whether it's time to update the HIPAA Security Rule itself - and not just the NIST guidance.

"The HIPAA Security Rule is a very process-oriented rule, by intent," says privacy attorney Kirk Nahra of the law firm WilmerHale.

"It addresses ways to think about and approach security, rather than identify specific standards to follow. That means that, from my perspective, it is in many ways a perfect rule that does not need to be updated in its language - the [compliance] process must be updated regularly by any covered entity or business associate, but that 'updating' is already incorporated into the rule."

NIST is trying to give organizations "a way to turn the HIPAA process into reality - to move from process to substance," with updated guidance, he contends.

If HHS were to consider changes to the HIPAA Security Rule, "I would only caution them as they move through the process of evaluating potential changes to keep the idea of the HIPAA Security Rule as it is, and not to turn a broad process that is flexible and scalable to adjust to the wide volume of different kinds of entities regulated by HIPAA into something more specific and less flexible," Nahra says.

Read the rest here:

https://www.govinfosecurity.com/nist-seeks-input-on-hipaa-security-rule-guidance-update-a-16519?&web_view=true

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
Information Systems Security Association
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
Information Systems Security Association
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 to Defense Sector: Think Twice Before Connecting Operational Technology to the Internet

By Mariam Baksh, NextGov, April 30, 2021

The agency recognized benefits such as enabling remote work but notes the inherent risks and costs of putting industrial control system components online.

Given recent intrusions, the National Security Agency warns organizations should reassess the pros and cons of connecting the operational technology in their industrial control systems to information technology and the public internet.

"Acknowledge that a standalone, unconnected ('islanded') OT system is safer from outside threats than one connected to an enterprise IT system(s) with external connectivity (no matter how secure the outside connections are thought to be)," reads the first step in a guide the agency released Thursday for evaluating such systems.

The guide applies to network owners within the National Security System, the Defense Department and the defense industrial base, where NSA said malicious cyber activity continues to target the operational technology such as valves and pressure sensors that control physical processes in industrial operations and can have consequences such as loss of life if compromised.

This operational technology predates the internet but operators have connected it to information technology over the years in order to benefit from the ability to process data, leverage the IT workforce, monitor the systems and manage updates. But the NSA said entities have not paid enough attention to the cybersecurity risks involved, and it's time for a change in their approach.

"A significant shift in how operational technologies are viewed, evaluated, and secured within the U.S. is needed to prevent malicious cyber actors from executing successful, and potentially damaging cyber effects. As OT components continue being connected to information technology, IT exploitation increasingly can serve as a pivot to OT destructive effects," according to the guide. "While OT systems rarely require outside connectivity to properly function, they are frequently connected for convenience without proper consideration of the true risk and potential adverse business and mission consequences."

Read the rest here:

https://www.nextgov.com/cybersecurity/2021/04/nsa-defense-sector-think-twice-connecting-operational-technology-internet/173740/

DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized

By Brian Krebs, Krebs on Security, May 14, 2021

The **DarkSide** ransomware affiliate program responsible for the six-day outage at **Colonial Pipeline** this week that led to fuel shortages and price spikes across the country is running for the hills. The crime gang announced it was closing up shop after its servers were seized and someone drained the cryptocurrency from an account the group uses to pay affiliates.

"Servers were seized (country not named), money of advertisers and founders was transferred to an unknown account," reads a message from a cybercrime forum reposted to the Russian OSINT Telegram channel.

"A few hours ago, we lost access to the public part of our infrastructure," the message continues, explaining the outage affected its victim shaming blog where stolen data is published from victims who refuse to pay a ransom.

"Hosting support, apart from information 'at the request of law enforcement agencies,' does not provide any other information," the DarkSide admin says. "Also, a few hours after the withdrawal, funds from the payment server (ours and clients') were withdrawn to an unknown address."

DarkSide organizers also said they were releasing decryption tools for all of the companies that have been ransomed but which haven't yet paid.

Read the rest here:

https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/

Joint CISA-FBI Cybersecurity Advisory on DarkSide Ransomware

05/11/2021 01:42 PM EDT

CISA and the Federal Bureau of Investigation (FBI) have released a Joint Cybersecurity Advisory (CSA) on a ransomware-as-a-service (RaaS) variant—referred to as DarkSide—recently used in a ransomware attack against a critical infrastructure (CI) company.

Cybercriminal groups use DarkSide to gain access to a victim's network to encrypt and exfiltrate data. These groups then threaten to expose data if the victim does not pay the ransom. Groups leveraging DarkSide have recently been targeting organizations across various CI sectors including manufacturing, legal, insurance, healthcare, and energy.

Prevention is the most effective defense against ransomware. It is critical to follow best practices to protect against ransomware attacks, which can be devastating to an individual or organization and recovery may be a difficult process. In addition to the Joint CSA, CISA and FBI urge CI asset owners and operators to review the following resources for best practices on strengthening cybersecurity posture:

CISA and Multi-State Information Sharing and Analysis Center: Joint Ransomware Guide

CISA webpage: Ransomware Guidance and Resources

CISA Insights: Ransomware Outbreak

CISA Pipeline Cybersecurity Initiative

CISA Pipeline Cybersecurity Resources Library

Victims of ransomware should report it immediately to CISA, a local FBI Field Office, or a Secret Service Field Office.

DefakeHop: A deepfake detection method that tackles adversarial threat detection and recognition

By Staff, HelpNet Security, May 7, 2021

Army researchers developed a deepfake detection method that will allow for the creation of state-of-the-art soldier technology to support mission-essential tasks such as adversarial threat detection and recognition.

This work specifically focuses on a lightweight, low training complexity and high-performance face biometrics technique that meets the size, weight and power requirements of devices soldiers will need in combat.

Researchers at the U.S. Army Combat Capabilities Development Command, known as DEVCOM, Army Research Laboratory, in collaboration with Professor C.-C. Jay Kuo's research group at the University of Southern California, set out to tackle the significant threat that deepfake poses to our society and national security. The result is an innovative technological solution called DefakeHop.

Deepfake detection with DefakeHop

Deepfake refers to artificial intelligence-synthesized, hyper-realistic video content that falsely depicts individuals saying or doing something, said ARL researchers Dr. Suya You and Dr. Shuowen (Sean) Hu. Most state-of-the-art deepfake video detection and media forensics methods are based upon deep learning, which have many inherent weaknesses in terms of robustness, scalability and portability.

"Due to the progression of generative neural networks, AI-driven deepfake advances so rapidly that there is a scarcity of reliable techniques to detect and defend against deepfakes," You said. "There is an urgent need for an alternative paradigm that can understand the mechanism behind the startling performance of deepfakes and develop effective defense solutions with solid theoretical support."

Read the rest here:

https://www.helpnetsecurity.com/2021/05/07/defakehop-deepfake-detection-method/?web_view=true

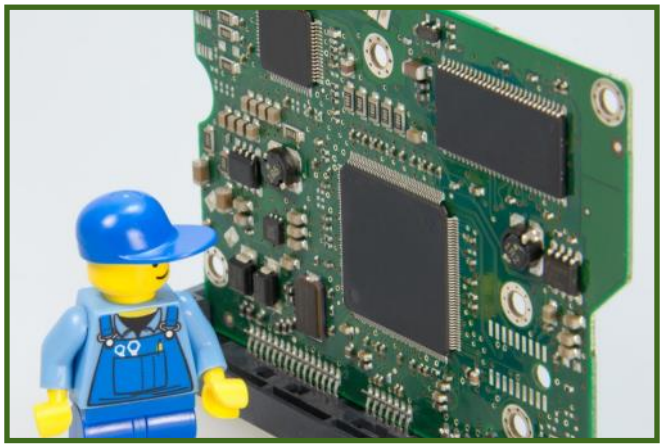
The global chip shortage will be a long-lasting problem. Here's what it means for you, and for the world

By Daphne Leprince-Ringuet , ZDNet, May 12, 2021

If you were hoping to get your hands on a new smartphone, or pondering whether to renew your PC, you might want to think again: according to research firm Gartner, the global chip shortage that is hitting a number of sectors isn't set to subside before well into 2022.

Severe semiconductor shortages will persist throughout 2021, with recovery only starting towards the end of the year to reach normal levels from the second quarter of 2022 onwards, says Gartner. By that time, new manufacturing capacity will help ease the situation.

Meanwhile, however, the time it takes to produce a chip could increase by six months, and even up to a year for more specific semiconductors. Key devices to be impacted will include power management chips, CMOS image and touch sensors, as well as fingerprint sensors and microcontrollers.



Gartner identifies a number of reasons that explain the current shortage. The first one is geopolitical: with tensions between the US and China escalating in recent months, Chinese tech companies have been stockpiling record amounts of chips and chip-making equipment.

At the same time, some key semiconductor manufacturers had to temporarily suspend production. In Austin, Texas, Samsung shut down a chip plant for more than a month because of power outages arising from blistering cold weather; and in Japan, Renesas recently paused production following the outbreak of a fire on-site.

Still, the situation could have been manageable – had a global pandemic not prompted consumers and businesses around the world to frantically buy new devices to remain connected to friends, families and colleagues while the health crisis locked entire populations inside their homes for months on end.

Shipments of PCs, tablets and gaming consoles soared in the past year; while smartphone sales didn't pick up as fast, it is expected that consumers will be keen to switch their handsets to 5G-enabled devices in 2021, and demand for mobile phones is set to skyrocket in the coming months.

All those devices are powered and controlled by semiconductors, and in fact, chip sales grew to a mammoth $464 billion in 2020, an increase of 11% compared to 2019.

At first glance, the numbers seem to reflect a healthy and thriving industry. But in reality, semiconductor manufacturing facilities – typically called "foundries", or "fabs" – are struggling to cope with such heightened demand, and the pace of production is rapidly falling behind.

The Chip Supply Chain: A Global Journey

The semiconductor supply chain is an unusual one. Some companies, like Intel, design and manufacture their own chips, and as such are known as Integrated Device Manufacturers (IDMs). Others, like Nvidia, only design semiconductors without manufacturing them: they are called "fabless".

And then, there are companies that run fabs where anybody and everybody can place an order. This is the case of a handful of companies, the most established of which are Samsung and TSMC.

"There are a couple of very big IDMs at the moment," Alan Priestley, Europe semiconductor analyst at Gartner, tells ZDNet. "But most of the industry relies on the use of foundries, and the reason this has happened is because it is massively expensive to build semiconductor manufacturing facilities."

Intel is an exception, says Priestley: through continuous investment, the company has managed to establish itself as a major chip designer and manufacturer. But for the majority of businesses, it is still necessary to delegate semiconductor manufacturing to external foundries.

Read the rest here:

https://www.zdnet.com/article/the-global-chip-shortage-will-be-a-long-lasting-problem-heres-what-it-means-for-you-and-for-the-world/

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.

How to Tell a Job Offer from an ID Theft Trap

By Brian Krebs, Krebs on Security, May 21, 2021

One of the oldest scams around — the fake job interview that seeks only to harvest your personal and financial data — is on the rise, the **FBI** warns. Here's the story of a recent **LinkedIn** impersonation scam that led to more than 100 people getting duped, and one almost-victim who decided the job offer was too-good-to-be-true.

Last week, someone began posting classified notices on LinkedIn for different design consulting jobs at Geosyntec Consultants, an environmental engineering firm based in the Washington, D.C. area. Those who responded were told their application for employment was being reviewed and that they should email Troy Gwin — Geosyntec's senior recruiter — immediately to arrange a screening interview.

Gwin contacted KrebsOnSecurity after hearing from job seekers trying to verify the ad, which urged respondents to email Gwin at a Gmail address that was not his. Gwin said LinkedIn told him roughly 100 people applied before the phony ads were removed for abusing the company's terms of service.

"The endgame was to offer a job based on successful completion of background check which obviously requires entering personal information," Gwin said. "Almost 100 people applied. I feel horrible about this. These people were really excited about this 'opportunity'."

Erica Siegel was particularly excited about the possibility of working in a creative director role she interviewed for at the fake Geosyntec. Siegel said her specialty — "consulting with start ups and small businesses to create sustainable fashion, home and accessories brands" — has been in low demand throughout the pandemic, so she's applied to dozens of jobs and freelance gigs over the past few months.

On Monday, someone claiming to work with Gwin contacted Siegel and asked her to set up an online interview with Geosyntec. Siegel said the "recruiter" sent her a list of screening questions that all seemed relevant to the position being advertised.

Siegel said that within about an hour of submitting her answers, she received a reply saying the company's board had unanimously approved her as a new hire, with an incredibly generous salary considering she had to do next to no work to get a job she could do from home.

Worried that her potential new dream job might be too-good-to-be-true, she sent the recruiter a list of her own questions that she had about the role and its position within the company.

But the recruiter completely ignored Siegel's follow-up questions, instead sending a reply that urged her to get in touch with a contact in human resources to immediately begin the process of formalizing her employment. Which of course involves handing over one's personal (driver's license info) and financial details for direct deposit.

Multiple things about this job offer didn't smell right to Siegel.

"I usually have six or seven interviews before getting a job," Siegel said. "Hardly ever in my lifetime have I seen a role that flexible, completely remote and paid the kind of money I would ask for. You never get all three of those things."

So she called her dad, an environmental attorney who happens to know and have worked with people at the real Geosyntec Consultants. Then she got in touch with the real Troy Gwin, who confirmed her suspicions that the whole thing was a scam.

"Even after the real Troy said they'd gotten these [LinkedIn] ads shut down, this guy was still emailing me asking for my HR information," Siegel said. "So my dad said, 'Troll him back, and tell him you want a signing bonus via money order.' I was like, okay, what's the worst that could happen? I never heard from him again."

HOW TO SPOT A JOB SCAM

In late April, the FBI warned that technology is making these scams easier and more lucrative for fraudsters, who are particularly fond of impersonating recruiters.

Read the rest here:

https://krebsonsecurity.com/2021/05/how-to-tell-a-job-offer-from-an-id-theft-trap/

WWW.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: April Frost
IT Committee: Patrick Sheehan
Speaker's Bureau: Kelli Blanchard
Girl Scouts Cyber Badge Camp: Anna Parrish
Annual Election: Colleen Murphy

**** Executive Board Members***

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

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

Time For A Change

By Don Creamer, ISSA-COS, May 31, 2021

I apologize that this is not one of the quirky articles that normally graces this space. I am using my Editor's privilege a final time to write a personal note.

This is the last issue of the ISSA-COS Newsletter I shall be publishing. After nine and half years it is time for a change in the editorship of this periodical.

My replacement has been chosen by the Board (I turned in my notice in January), and I hope that you will be pleased with the planned changes.

Respectfully,