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

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 10 NUMBER 3 MARCH 2021

Off to a Great Start!

A Note From Our President

By Mr. Ernest Campos

With two full months of 2021 now behind us, I must say it feels good to be back to our normal schedule of events. So far, we are off to a great start! As with every new year, we often encounter a few glitches needing to be adjusted, gaps in our communications, or area we can improve upon. Notwithstanding such calibrations, our team of board members and key personnel are hard at work keeping the lights on for our chapter.

Hopefully, many of you were able to attend the presentation provided by **Mr. Chris Gorog** (CEO, BlockFrame) during our February chapter meeting. Chris' presentation was entitled: "*Future Directions in Privacy Enabling Technology*" and provided us with an update on the latest news and developments surrounding blockchain technologies. At our February events, we also announced the return of Murray Security Services (MSS) as a 3-time Platinum sponsor to our chapter. The financial contributions provided by MSS and **Dr. Shawn Murray** (CEO), **Ms. Shelly Murray** (COO), and **Ms. Abbey Murray** (the one who really gets things done will help ensure our chapter's ability to cover the cost of operations throughout the year to come.

In addition to renewing their sponsorship, MSS has also initiated a new Strategic Partnership with our chapter. This partnership will privilege the members of our chapter to incredible benefits in the areas of training and professional benefits. Here is a summary of the benefits our members gain from this partnership.

- $10,000 cash commitment to ISSA-COS to be applied to our annual operating costs
- $1,000 discount on all MSS Professional Training & Certification courses; an exclusive offer for members of ISSA-COS only
- 4 free subscriptions to EC-Council's **CODERED** video training catalog to be raffled off throughout the year
- 1 free training seat for EC-Council's **Certified Threat Intelligence Analyst (CTIA)** to be raffled off during the year

(Continued on page 4)

Why Russia Is Terrified of SpaceX -- and Starlink

By Rich Smith, The Motley Fool, February 15, 2021

SpaceX wants to bring fast satellite broadband internet to the world -- and in particular, to internet users in far-flung, rural locations, where download speeds are low and prices are high.

One of the first places in America to get SpaceX Starlink service was Alaska, the state with the lowest population density in the country -- just one person per square mile. The company next extended service into Canada (population density: three people per square mile), followed last month by service in the UK -- a big jump in concentration, with 650 people per square mile. (Even in the UK, there are plenty of isolated locations where internet service is expensive, slow -- or both).

"Despite having heavy urbanization in its western parts, 1 in 4 Russians still lives in the countryside, making the country more rural than even the U.S., for example, where only 1 in 6 people live outside urban locales. "

SpaceX's globe-spanning satellite constellation should be capable of providing 100 megabit-per-second internet service to *anywhere* by the end of this year. You can expect that a lot of countries, no matter how urbanized they are (or not), will be lining up to sign up for Starlink service. And the more countries Starlink signs up as customers, the better the prospects for the SpaceX subsidiary's promised IPO.

One country that most definitely does *not* want Starlink, however, is Russia.

Just say "nyet" to fast internet

As ArsTechnica.com reported last month, the Russian State Duma (Russia's congress) is currently considering legislation to impose fines upon any individual or company that signs up for Starlink -- or indeed, for any foreign-operated satellite internet system, OneWeb or Project Kuiper included. According to ArsTechnica, the Russian Duma may fine individual customers of Starlink up to $405 for use of the satellite internet service, and fine corporate users as much as $13,500.

What does Russia have against cheap, fast, reliable internet from space? For one thing, Russian security services object that internet operated by a foreign satellite network would be immune from surveillance under Russia's System of Operational Search Measures legislation ("SORM"). For another, they suspect that Starlink is part of a U.S. government plot to deploy "predatory, clever, powerful, high-technology ... shock and awe ... to advance, above all, [American] military interests."

Yes, seriously.

And yet, there also seems to be an economic motivation to this ban on Starlink and other satellite networks. As Ars points out, "Russia is planning its own satellite Internet constellation, known as 'Sphere.'" And in contrast to SpaceX's Starlink, which is a privately funded and privately built communications system, the 600-satellite Sphere constellation will be a project built and run by the Russian state under the aegis of its Roscosmos space agency. And that could be a problem.

Sphere, you see, is rumored to cost $20 billion to build, may not begin launching until 2024, and won't be completed before 2030. Given the amount of investment required, Russia's government certainly doesn't want to pay for the Sphere project only to discover three years from now that all of Sphere's potential customers have already signed up for Starlink -- and that it will never recover its investment.

That problem goes away, however, if Russia takes the simple step of banning competitors from its market.

What it means for SpaceX

Read the rest here:

https://www.fool.com/investing/2021/02/15/why-russia-is-terrified-of-spacex-and-starlink/

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 ~351 members as of the end of December 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.

Thanks,

Craig Westerfield

VP-Membership
membership@issa-cos.org

New Members February 2021	
Dr. Kelly Hughes	Mrs. Shelley Murray
Mr. Joseph Karpp	Mr. Eric Johnson
Mr. Joseph Cheung	Mr. Michael Wellman
Mr. Ryan Paugh	

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

A Note From Our President

(Continued from page 1)

- 1 free training seat for EC-Council's **Certified Security Analyst (ECSA): Penetration Testing** to be raffled off during the year

As we inch closer to the end of the first quarter of the year, we remain hopeful we will soon be able to resume in-person events. Rest assured, we will not rush this decision and we will retain a virtual option for as many of our events as possible. Until then however, we will continue to fully utilize our virtual platforms to keep our schedule of events moving forward.

Looking forward towards March, registration is underway for our Spring Virtual Security+ Review. This three Saturday event will take place on 3/6, 3/13, and 3/20. Registration is free for members of ISSA-COS and we encourage attendance for non-members hoping to gain their interest in joining our chapter. So, if you know of someone looking to sharpen the knowledge of Information Security and is preparing to take the CompTIA Security+ CE exam, invite them to register and participate.

Also coming soon is our annual Cyber Focus Symposium which has moved to April this year. Extra time was needed to switch this event to a fully virtual platform. Registration will soon open and my preview of scheduled speakers suggests this will be a great event. Please help spread the word and encourage everyone within our community to register to attend.

In closing, I thank all our members for their continued support of our chapter even in the still challenging times in which we are living. It because of our strong and dedicated membership that we can attract valuable sponsors, strategic partners, and nationally recognized guest speakers. It is also our members who create our wealth of knowledge, vast skill sets, and depth of years of service to our community. All of you are appreciated and well-respected professionals and we are a blessed chapter to have you in it.

Sincerely,

Ernest

ISSA-COS Sponsorship Plans

ISSA Colorado Springs Chapter

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

Book(s) Report

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

Our 2020 ISSA-COS chapter meeting presenters recommended these two books:

- Kim, Gene, Kevin Behr, and George Spafford. *The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win*. 5th Anniversary Edition. Portland, OR: IT Revolution, 2018, first published in 2013.
- Kim, Jean. *The Unicorn Project: A Novel about Developers, Digital Disruption, and Thriving in the Age of Data*. IT Revolution Press, 2019.

I read them, I see the value, and I recommend them as well, read in the sequence published, as they are interconnected.

Why do I think they are worth your time?

First, they are quite readable yarns, even when you are tired and the last thing you want to read is another technical book. They are good stories, not just textbooks or reference books. That is not to take away from their valuable information about the IT and cybersecurity world!

You can get them together online in hardcopy for about 30 bucks, probably less if you use e-readers. They are also available through the Pikes Peak Library system. If you are cheap like me, there is no financial excuse for not having read them. The editions I have are 431 pages and 342 pages, respectively. There is little-to-no passive voice. Their Flesh readability score is about 65.5 or Flesh-Kincaid readability grade level 7.5, easier to read than a typical newsmagazine. Unfortunately, you will find my writing in this article is less readable than the books!

You can pick them up, read a few pages, and put them down, or read them while the family is watching TV. You will find yourself reading a bit more than that at a time, as the storylines are intriguing!

This is not your grade-school book report, where the student, at least in part, is trying to prove they actually read the book(s). I am interested in you enjoying the books as you consider their utility for you. The authors state in *The Unicorn Project* you do not have to read *The Phoenix Project* first to appreciate *The Unicorn Project*. Well, if they say so! For me, *The Phoenix Project* has more general management skills and knowledge embedded in the story, and *The Unicorn Project* is more current with today's business challenges.

The storylines concern a multi-billion-dollar traditionally non-IT manufacturer and retail company, first trying to survive in an IT world, then trying to get ahead. The characters are believable, and are both good 'good' examples, and good, 'bad' examples. Have you ever:

1) Worked for a boss that seems to only be interested in immediate problem - IT fixes, and not at all interested in creating an IT environment that long-term keeps a problem from creating repeated disruptions?
2) Been in a situation where lack of sleep or a lousy workspace environment compounded IT errors, yet management scorned the very idea of employee rest or quality workspace?
3) Run into ruthless, amoral bureaucrats than are not above weaponizing HR to take out their perceived opponents?
4) Been in organizations where there is one person with single-point-of-failure knowledge and skills, so that if that person is not available the system collapses?
5) Seen the single-point-of-failure person is recognized as such by their supervisor, but the supervisor is stymied in trying to improve the situation?
6) Seen a situation where cybersecurity pros are considered by the rest of IT to be naysayers or villains?
7) Seen unreasonable IT risks taken by non-IT knowledgeable senior leadership, and then they are outraged by the predictable IT failure?

Hey Jay! Enough of the human interest! Isn't there any good IT tech stuff?

Indeed, there is, especially about creating secure virtual environments to extensively test software before deployments. There is some coding storyline as well!

What I especially enjoyed was the material about how the cybersecurity professionals can be perceived by their mainstream IT teammates, either positively or negatively. The lesson I took home is it is not enough for us to be really good people, we must be perceived by our non-cybersecurity teammates as really good people, to be effective!

Good reading!

We're not bulletproof

By Scott Frisch, Executive Vice President, ISSA-COS

Now a Public Service Announcement: STRESS is real. The outcome of not addressing stress can be very permanent. I was one of those people that thought I was 10-feet tall and bulletproof and bad things happen to others. Until 2019. In 2019 I got a tap on the shoulder – a rude awakening that I wasn't bulletproof – and ended up in the hospital for a day with cardiac issues. Barely one year later I got a second tap on the shoulder – and heard these words from my doctor: "You have two choices, you can go to the hospital right now – or you can go home and die". This "tap on the shoulder" resulted in surgery and a 16-day hospital stay.

After numerous tests, and extensive poking and prodding, the doctors couldn't find a definitive cause for my cardiac issues. Until, that is, I described my 40-plus years of work. Burning the candle at both ends, as well as in the middle, and also not eating or sleeping well. For years I had been taking on the responsibilities of others, doing everything I possibly could to move projects and programs along. And getting frustrated – and stressed – at the lack of progress made by others.

The doctors told me bluntly – I was in the hospital because of stress. Period. Nothing else was wrong with me. Stress very nearly killed me. Those 16 days in 2020 became a life-changing event. I am now reminded, every single day, that I am not 10-feet tall and bulletproof. I needed to make significant changes, and embrace a good work/life balance, or not be here at all.

I recovered and now have a good work/life balance. Many thanks go out to so many people for their support and well wishes during my recovery. Thank you. One of the cyber phrases we all use is: if you see something, say something. It may save someone. End of the Public Service Announcement and back to the beginning of this article: Your job is not to herd the cats – your job is to identify the cats to be herded. This quote and work/life balance applies to everyone.

Take care.

Researcher hacks over 35 tech firms in novel supply chain attack

By Ax Sharma, Bleeping Computer, February 9, 2021

A researcher managed to breach over 35 major companies' internal systems, including Microsoft, Apple, PayPal, Shopify, Netflix, Yelp, Tesla, and Uber, in a novel software supply chain attack.

The attack comprised uploading malware to open source repositories including PyPI, npm, and RubyGems, which then got distributed downstream automatically into the company's internal applications.

Unlike traditional typosquatting attacks that rely on social engineering tactics or the victim misspelling a package name, this particular supply chain attack is more sophisticated as it needed no action by the victim, who automatically received the malicious packages.

This is because the attack leveraged a unique design flaw of the open-source ecosystems called **dependency confusion.**

For his ethical research efforts, the researcher has earned well over $130,000 in bug bounties.

Malware is distributed downstream automatically

Last year, security researcher Alex Birsan came across an idea when working with another researcher Justin Gardner.

Gardner had shared with Birsan a manifest file, *package.json*, from an npm package used internally by PayPal.

Birsan noticed some of the manifest file packages were not present on the public npm repository but were instead PayPal's privately created npm packages, used and stored internally by the company.

On seeing this, the researcher wondered, should a package by the same name exist in the public npm repository, in addition to a private NodeJS repository, which one would get priority?

Read the rest here:

https://www.bleepingcomputer.com/news/security/researcher-hacks-over-35-tech-firms-in-novel-supply-chain-attack/

STIG Update - STIG Update - Group Policy Objects have been updated

Group Policy Objects (GPOs) have been updated to include Microsoft Edge and to revise the Google Chrome files. See the Change Log document included in the zip file for additional information.

The DISA Risk Management Executive posts the GPOs for use by system administrators to ease the burden in securing systems within their environment.

The GPOs can be found on the Cyber Exchange website on the Group Policy Objects tab at https://cyber.mil/stigs/gpo/. For users who do not have a CAC that has DoD Certificates, the GPO is also available from https://public.cyber.mil/stigs/gpo/.

If you are not able to find and download the content, please report broken link issues to the DoD Cyber Exchange Web team at dod.cyberexchange@mail.mil. For all questions related to the STIG/SRG content itself, please contact the DISA STIG Customer Support Desk at disa.stig_spt@mail.mil.

STIG Update - DISA has released STIG Viewer Version 2.12

This latest version of STIG Viewer is available at https://public.cyber.mil/stigs/srg-stig-tools/

To accommodate rule identifier changes, this version of the STIG viewer allows for more flexible rule matching when importing data. These settings have been enabled by default, but may be disabled in Preferences. Consult section 2.2.4 ("Options") of the User Guide for additional information.

If you are not able to find and download the content, please report broken link issues to the DoD Cyber Exchange Web team at dod.cyberexchange@mail.mil. For all questions related to the STIG/SRG content itself, please contact the DISA STIG Customer Support Desk at disa.stig_spt@mail.mil.

Update Your Profile!

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

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.

ISSA Colorado Springs Chapter

Professional Development Options

- **Strategic Partnerships**
  - NEW! Murray Security Services (MSS)
  - National Cyber Exchange (NCX)
  - Info-Tech Research Group
  - Discover Goodwill
  - International Association of Privacy Professionals (IAPP)
- **Chapter Services**
  - Mentoring Program
  - Security + and CISSP Certification Reviews
  - Listings of Employment Opportunities
  - Online and In-person Networking Events
  - Courtesy Reminders for Membership Renewals

MURRAY SECURITY SERVICES
INFORMATION & CYBER SECURITY TRAINING & CONSULTING

NATIONAL CYBER EXCHANGE NCX

Discover Goodwill
Southern & Western Colorado

INFO~TECH RESEARCH GROUP

iapp

Strategic Partnership

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Murray Security Services Sponsorship

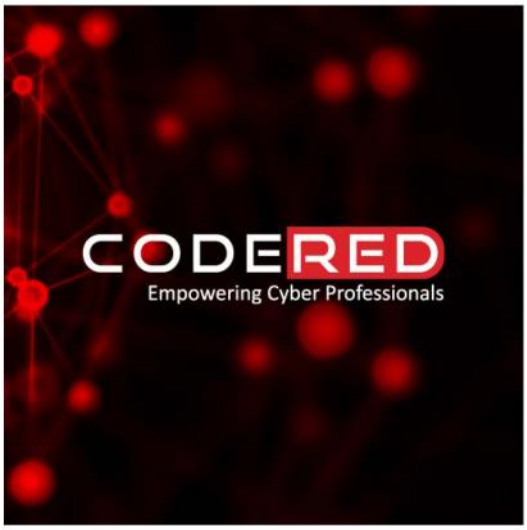
- $2,500 per quarter = $10,000 commitment
- 4 **CODERED** Licenses to be provided as give-always at ISSA-COS Events ($1000 value)
- $1000 off (preferred pricing) on most all MSS Professional Training & Certification courses. (no-one else receives this type of standard discount)
- Providing 2 (free) training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

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.

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

Spring Security + Review – Mar 6, 13, and 20, 2021

- Virtual Platform with Live Instructors and Live Q&A
- Personal Study Guide Included

April Chapter Meeting – 4/6/2021

- Chapter Announcements
- Technical Presentation

April Mini Seminar – 4/10/2021

- Technical Training
- Hands-on Tools and Techniques

Cyber Focus Symposium (CFS) – Apr 20, 21, and 22, 2021

- CFS Job Fair: *Sponsored by Cleared Careers*
- CFS CTF: *Sponsored by Splunk> and Epoch Concepts*
- CFS Conference: *Produced by Secret Sauce 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

9

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

Kia Motors America suffers ransomware attack, $20 million ransom

By Lawrence Abrams, Bleeping Computer, February 17, 2021

Kia Motors America has suffered a ransomware attack by the DoppelPaymer gang, demanding $20 million for a decryptor and not to leak stolen data.

Kia Motors America (KMA) is headquartered in Irvine, California, and is a Kia Motors Corporation subsidiary. KMA has nearly 800 dealers in the USA with cars and SUVs manufactured out of West Point, Georgia.

Yesterday, we reported that Kia Motors America was suffering a nationwide IT outage that has affected their mobile UVO Link apps, phone services, payment systems, owner's portal, and internal sites used by dealerships.

When visiting their sites, users are met with a message stating that Kia is "experiencing an IT service outage that has impacted some internal networks," as shown below.

A Kia owner tweeted that when they attempted to pick up their new car, a dealership told them that the servers were down due to a ransomware attack.

> @Kia I went to the Kia dealership in Arizona and signed a new lease, yet the manager told me your computers have been down for 3 days due to Ransomware and has affected Kia all over the USA. Can't get my car for ???? Now what?
>
> — Amybean (@amylee62) February 16, 2021

When we contacted Kia Motors America yesterday about these outages and ransomware reports, KMA told us that they were working on resolving the outage.

"KMA is aware of IT outages involving internal, dealer and customer-facing systems, including UVO. We apologize for any inconvenience to our customers and are working to resolve the issue and restore normal business operations as quickly as possible." - Kia Motors America.

Today, BleepingComputer obtained a ransom note that we were told was created during an alleged Kia Motors America cyberattack by the DoppelPaymer ransomware gang.

In a ransom note seen by BleepingComputer, the attackers state that they attacked Hyundai Motor America, Kia's parent company. Hyundai does not appear to be affected by this attack.

The ransom note contains a link to a private victim page on the DoppelPaymer Tor payment site that once again states the target is 'Hyundai Motor America.'

The Tor victim page says that a "huge amount" of data was stolen, or exfiltrated, from Kia Motors America and that it will be released in 2-3 weeks if the company does not negotiate with the threat actors.

DoppelPaymer is known for stealing unencrypted files before encrypting devices and then posting portions on their data leak site to further pressure victims into paying.

To prevent the leak of the data and receive a decryptor, DoppelPaymer is demanding 404 bitcoins worth approximately $20 million. If a ransom is not paid within a specific time frame, the amount increases to 600 bitcoins, or $30 million.

The DoppelPaymer operation has not indicated what type of data has been stolen. Based on the amount of Kia services suffering an outage, we can expect a wide range of affected servers.

The stealing of unencrypted files has become a widely used tactic by ransomware operations to coerce victims to pay, with Emsisoft stating it has affected more than 1,300 companies globally.

"Globally, more than 1,300 companies, many US-based, lost data including intellectual property and other sensitive information. Note, this is simply the number of companies which had data published on leak sites and takes no account of the companies which paid to prevent publication," states Emsisoft's 2020 State of Ransomware report.

Read the rest here:

https://www.bleepingcomputer.com/news/security/kia-motors-america-suffers-ransomware-attack-20-million-ransom/

Technology Executives Say All Evidence Points To Russia In Major Hack Of Computer Networks

By Staff, Radio Free Europe/Radio Liberty, February 24, 2021

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.

The hearing was the first to examine the hack, which was discovered by private security company FireEye in December. It was later revealed that hackers slipped malicious code into updates of network-management software made by the U.S. company SolarWinds, which was then downloaded by several branches of the U.S. government and several U.S. and European corporations.

U.S. intelligence officials and industry sources had previously blamed the intrusion on Russian hackers. Moscow has denied any involvement.

But the technology executives said that the evidence points to Russia as they described the precision, ambition, and scope of the attack.

"We asked ourselves how many engineers do we believe had worked on this collective effort. And the answer we came to was...at least 1,000, very skilled, capable engineers," Microsoft President Brad Smith told the Senate Intelligence Committee.

"We've seen substantial evidence that points to the Russian foreign intelligence agency and we have found no evidence that leads us anywhere else," Smith said.

Smith told the committee that the true scope of the intrusions is still unknown because most victims are not legally required to disclose attacks unless they involve sensitive information about individuals.

President Joe Biden's administration is weighing punitive measures against Russia, and White House press secretary Jen Psaki said it would be "weeks not months" before the U.S. responds.

"We have asked the intelligence community to do further work to sharpen the attribution that the previous administration made about precisely how the hack occurred, what the extent of the damage is, and what the scope and scale of the intrusion is," Psaki said. "And we're still in the process of working that through now."

At least nine government agencies and 100 private companies were breached, but what was taken has not been revealed. U.S. government agencies affected include the Treasury, Justice, and Commerce departments, but the full list has not been publicly released.

Smith said there are victims around the world, including in Canada, Mexico, Spain, and the United Arab Emirates.

Microsoft revealed in December that the hackers were able to gain access into its closely guarded source code but said they did not have permission to modify any code or engineering systems.

FireEye CEO Kevin Mandia told the Senate committee that his company has nearly 100 people working to study and contain the breach.

He said the hackers first installed malicious code in October 2019 but didn't activate it immediately in order to see if they could remain undetected. They then returned in March and began to steal the log-in credentials of people who were authorized to be on the networks so they could have a "secret key" to move around at will, Mandia said.

Read the rest here:

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

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.

Chapter Officers:

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

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

Dir. of Professional Outreach: Katie Martin
- Deputy: **Vacant**

Director of Communications : Christine Mack
- Deputy: Ryan Evan

Director of Certifications: Derick Lopez
- Deputy: Luke Walcher

Vice President of Membership: Craig Westerfield
- Deputy: **Vacant**

Vice President of Training: Jeff Tomkiewicz
- Deputy: Phebe Swope

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: Mark Heinrich
Mentorship Committee Chair: Carissa Nichols
Media/Newsletter: Don Creamer
IT Committee: Patrick Sheehan
Speaker's Bureau: William (Jay) Carson
Girl Scouts Cyber Badge Camp: Anna Parrish
Annual Election: Colleen Murphy

**** Executive Board Members***

Article for the Newsletter?

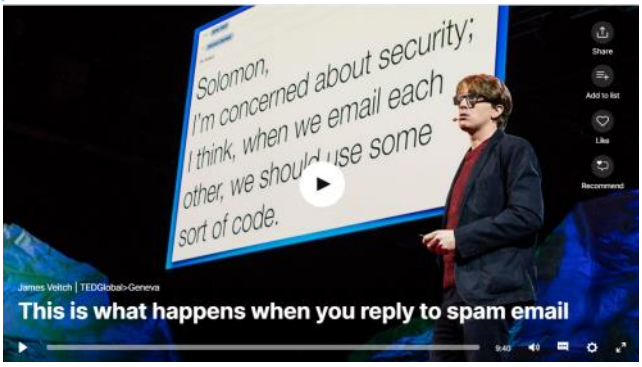
We are always looking for articles that may be of interest to the broader Colorado Springs cyber community.

Send your article ideas to the Newsletter at:

newsletter@issa-cos.org

Past Senior Leadership

President Emeritus: Dr. George J. Proeller
President Emeritus: Mark Spencer
Past President: Mike O'Neill
Past President: Pat Laverty
Past President: Cindy Thornburg
Past President: Frank Gearhart
Past President: Colleen Murphy



This is What Happens When You Reply to Spam Email

By James Veitch, TED, Undated

See the video here:

https://www.ted.com/talks/james_veitch_this_is_what_happens_when_you_reply_to_spam_email/transcript?language=en

Published at no cost to ISSA Colorado Springs by Sumerduck Publishing ™, Woodland Park, Colorado