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

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 9 NUMBER 12 DECEMBER 2020

"... and a partridge in a pear tree!"

A Note From Our President

By Mr. Ernest Campos

Welcome to December: Candles, Twinkling Lights, Candy Canes, and the hope of a better year to come in 2021. But, before we stick a fork in 2020, let us take a look at everything we have been doing to finish the year and what we are doing to prepare for the next one.

To kick-off November, we enjoyed an encore perform-ance from Mr. Michael Wyle, Director of Cybersecurity, Richie May Technology Services. Mr. Wyle resumed his discussion from earlier this year to complete his presentation on the "Intro to Malware Analysis and Response (MA&R)." Just like before, his presentation was very well received. Mr. Wyle has a gift to taking extremely complicated subjects and converting them to easy to understand discussions. If you missed his presentation, enjoy the playback from our chapter website – and collect CPE/CEU credits too!

In the heart of November, ISSA-COS hosted the 10th Annual (Virtual) Peak Cyber Symposium (produced by Secret Sauce Events, LLC in collaboration with Global Event Management, LLC). Despite the shift to a virtual format, the need to extend the duration of this event, and the pre-recorded presentations (yet, with live Q&A), both registration and participation were greater than we could have ever imagined. We received numerous compliments on the simple, clean layout of the Whova virtual platform. We even had many participants say Peak Cyber was the *best* virtual conference in all of 2020. Wow! What a compliment! The agenda for this event included the first Peak Cyber Job Fair, the return of the Peak Cyber Boss-of-the-NOC/Capture-the-Flag competetion (*Congrats to Andrew Funk for the win!*), and two full days of keynote speakers, breakout sessions, and panel discussions. If you missed this epic event, there is still time to enjoy all the presentations. Playbacks of all sessions will remain available for the next 6-months and all playbacks qualify for

(Continued on page 4)

How Facebook's AI Tools Tackle Misinformation

By Tekla S. Perry, IEEE Spectrum, November 19, 2020

Facebook today released its quarterly Community Standards Enforcement Report, in which it reports actions taken to remove content that violate its policies, along with how much of this content was identified and removed before users brought it to Facebook's attention. That second category relies heavily on automat-ed systems developped through machine learning.

"Schroepfer also reported that Facebook has deployed weapons to fight deep fakes. "

In recent years, these AI tools have been focused on hate speech. According to Facebook CTO Mike Schroepfer, the company's automated systems identified and removed three times as many posts containing hate speech in the third quarter of 2020 as in the third quarter of 2019. Part of the credit for that improvement, he indicated, goes to a new machine learning approach that uses live, online data instead of just offline data sets to continuously improve. The technology, tagged RIO, for Reinforced Integrity Optimizer, looks at a number tracking the overall prevalence of hate speech on the platform, and tunes its algorithms to try to push that number down.

"The idea of moving from a handcrafted off-line system to an online system is a pretty big deal," Schroepfer said. "I think that technology is going to be interesting for us over the next few years."

During 2020, Facebook's policies towards misinformation became increasingly tighter, though many would say not tight enough. The company in April announced that it would be directly warning users exposed to COVID-19 misinformation. In September it announced expanded efforts to remove content that would suppress voting and a plan to label claims of election victory before the results were final. In October it restricted the spread of a questionable story about Hunter Biden. And throughout the year it applied increasingly explicit tags on content identified as misinformation, including a screen that blocks access to the post until the user clicks on it. Guy Rosen, Facebook vice president of integrity, reported that only five percent of users take that extra step.

That's the policy. Enforcing that policy takes both manpower and technology, Schroepfer pointed out in a Zoom call with journalists on Wednesday. At this point, he indicated, AI isn't used to determine if the content of an original post falls into the categories of misinformation that violates its standards—that is a job for human fact-checkers. But after a fact-checker identifies a problem post, the company's similarity matching system hunts down permutations of that post and removes those automatically.

Facebook wants to automatically catch a post, says Schroepfer, even if "someone blurs a photo or crops it… but we don't want to take something down incorrectly."

"Subtle changes to the text—a no, or not, or just kidding—can completely change the meaning," he said. "We rely on third-party fact checkers to identify it, then we use AI to find the flavors and variants."

The company reported in a blog post that a new tool, SimSearchNet++, is helping this effort. Developed through self-supervised learning, it looks for variations of an image, adding optical character recognition when text is involved.

As an example, Schroepfer pointed to two posts about face masks identified as misinformation (above).

Read the rest here:

https://spectrum.ieee.org/view-from-the-valley/artificial-intelligence/machine-learning/how-facebooks-ai-tools-tackle-misinformation

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 ~325 members as of the end of October 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,

Steven Mulig

VP-Membership
membership@issa-cos.org

New Members November	
Samuel C Mercer	Larry OBrien
Tony Gooch	Atta Owusu Sarpong

Congratulations to the following ISSA International Award Winners:

Scott Frisch: **Honor Roll**

- 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.

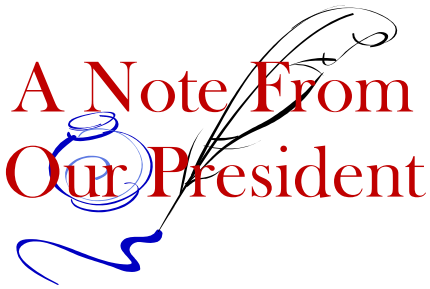
William (Jay) Carson: **Volunteer of the Year**

- The Volunteer 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.

Exceptional accomplishment by both!! Well done!

(Continued from page 1)

CPE/CEU credits! Visit www.peakcyberco.com for more information.



In November, ISSA-COS held its annual elections whereby we vote on the selection of 50% of our board members each year. In October we released a Call for Candidates. From among those who responded to the call, the following individuals were voted into office and will assume their roles on January 1st.

- President and Chair(person) of the Board: **Ernest Campos**
- Recorder/Historian: **Andrea Heinz**
- Vice President of Training: **Jeff Tomkiewicz**
- Director of Certification: **Derick Lopez**
- Director of Professional Outreach: **Katie Martin**
- Member-at-Large #3: **James Asimah**
- Member-at-Large #4: **Jay Carson**

Also, in November, ISSA International released the results of the Fellows Program and Annual Awards. Our chapter is blessed to have such active Past-Presidents who assist with developing the candidate packages for our members. Their efforts, especially those of Colleen Murphy, resulted in a strong showing for our chapter. The winners/recipients from our chapter include the following folks. If you know them or see them, be sure to congratulate them on a job well done!

- **ISSA International Fellows Program**
  - ⇒ ISSA International Senior Member: **Amy Coffman, Derick Lopez,** and **James Asimah**
  - ⇒ ISSA International Fellow: **Kurt Danis**
  - ⇒ ISSA International Distinguished Fellow: **Scott Frisch** and **Warren Pierce**
- **ISSA International Awards**
  - ⇒ ISSA International Volunteer of the Year: **Jay Carson**
  - ⇒ ISSA International Honor Roll: **Scott Frisch**

As we look forward to December, we still have two incredible events on our schedule before the year is over. On December 3rd, we will receive a special presentation from Mr. Jay Carson and Friends. The subject of their discussion is "*Cyber Bubble Wrap: How to apply cybersecurity to defend senior citizens.*" Then, on December 17th, our chapter will conclude the year with our Annual Chapter Celebration. During this event, we will honor all the accomplishments of our members, our chapter, and our community. The Keynote Speaker for this event will be Ms. Erin Miller who will provide us with an update on the Space ISAC (Information Sharing and Analysis Center).

Finally, in additional to everything that occurred over the last 30-days, behind the scenes we have been busy developing our agenda for 2021. So, what can we look forward to next year? How about the return of our monthly Chapter Meetings, Mini-Seminars, and Special Interest Groups? In 2021 we will also celebrate the 30-year anniversary of our chapter's existence and the introduction of the ISSA-COS Annual STAR Awards. It all starts with the Annual President's Address on Tuesday, January 5th. A full listing of 2021 events can be found in the December Newsletter.

In closing, despite all the challenges 2020 held, I am proud to say for our chapter, it was a great year. We overcame adversity. We instituted new, now permanent capabilities. We enabled professionals from across the nation to still receive access to quality professional programming and the ability to earn valuable CPE/CEU credits. I am proud to be associated with this chapter and its members. Together we are stronger. Together, we are ISSA-COS.

Sincerely,

Ernest

More Notes from the ISSA-COS Speakers Bureau

By Jay Carson, ISSA-COS Speakers Bureau

Is the ISSA-COS Online Program Meeting Your Needs?

As you know, the ISSA-COS team has successfully provided an online program of speakers to the chapter in lieu of the Cyber Focus Symposium, in-person chapter meetings and mini-seminars. From the April 2nd to the September 24th offering, we have been able to conduct 18 sessions, offering members up to 27 hours of potential continuing education credits. Not too bad!

President Ernest Campos, on behalf of the chapter, has thanked all the speakers and ISSA-COS team members who made this possible.

Normally, after in-person presentations attendees can exchange business cards for networking. We want to match that offering as much as possible with our online program. The purpose of this article is to summarize the presentations thus far (each synopsis provided by the presenters and/or ISSA-COS leadership) and give contact information if ISSA-COS members wish further contact with the speakers.

Where do we take this? Are you using online education, and/or do you prefer other online programs? How can we make YOUR ISSA-COS program more useful for YOU? Do you want the ISSA-COS Online Program to continue on a weekly, biweekly, or monthly or 'not at all' basis if in-person presentations continue to be postponed due to COVID-19? Please email your preferences to execvp@ISSA-COS.org and speakersbureau@ISSA-COS.org. Thanks!

The April-May program was detailed in a previous newsletter.

June

1. 4 June 2020: **Speakers:** Mr. Peter Archibald, Regional Manager, US Government Sector, Checkmarx. Featuring: Mr. Jeff Hsiao, Mr. Michael Lee, Mr. Jeffrey Armstrong.

Topic: The Application Security Journey. **Synopsis:** Checkmarx discussed Application Security Testing solutions, with a demonstration of the Application Security journey from the Cyber Assurance Team through to the Developer's IDE. **Contact:** Mr. Archibald can be reached at Peter.Archibald@checkmarx.com.

2. 11 June 2020: **Speaker:** Jeff Tomkiewicz, Security+, CEH, Former ISSA-COS Deputy VP of Training. **Topic:** Hands on Virtual Lab Training with TryHackMe! **Synopsis:** This presentation included a hands-on Capture-the-Flag (CTF) experience utilizing the site "TryHackMe." TryHackMe is an online platform that teaches cybersecurity through interactive virtual labs. Labs are for all skill levels and focus on theoretical and practical security. The setup process is easy and can be done from any browser. No additional equipment or VM's were needed and this also works on NIPR terminals. **Contact:** Mr. Tomkiewicz can be reached at tomkiewiczjeff@gmail.com.

3. 25 June 2020: **Speaker:** Ms. Nina Di Francisco, Director, Info-Tech Research Group. **Topic:** Info-Tech RG Strategic Partnership: Member Benefits. **Synopsis:** ISSA-COS welcomed Info-Tech Research Group as our newest Strategic Partner. In this presentation, Nina Di Francisco provided a summary of all the benefits being made available to the members of our chapter. **Contact:** Ms. Di Francisco can be reached at ndifrancisco@infotech.com. **Speaker:** Ms. Christine Coz, Senior Director and Principal Security Advisor, Info-Tech Research Group. **Topic:** Responsibly Resume IT Operations in the Office. **Synopsis:** Ms. Coz discussed how best to accept changes following a pandemic crisis. Responsibly resuming operations will not be a return to the past for many of us. Understanding the new risk paradigm, and normalizing the many quick changes made to accommodate the work-from-home strategy are new top priorities. Ms. Coz can be reached at ccoz@infotech.com.

July

4. 9 July 2020: **Speaker:** Frank Gearhart, C|CISO, CISSP, C|HFI, C|NDA. **Topic:** Quantum Cryptology and How it Impacts our Profession. **Synopsis:** Practical quantum computing—assuming it is achieved—will have tremendous impacts on our global information society and could help solve currently intractable problems. Quantum cryptology could break the encryption algorithms that protect our financial, commercial, industrial, defense, and individual data systems. But quantum cryptology depends on capable and stable quantum computing, which currently face significant challenges. This was a look at some of the current research in quantum cryptology, some recommendations, and what we might expect from quantum cryptology in the near future. **Contact:** Mr. Gearhart can be reached at frank.gearhart@outlook.com.

Short Subject**: Speaker:** Mr. Wally Magda. **Topic:** How does a Presidential Executive Order Secure the Bulk Power System? **Contact:** Mr. Magda can be reached at wladekco@comcast.net.

5. 23 July 2020: **Speaker:** Mr. Nick Tate. **Topic:** The Tor Project. **Synopsis:** Just like Tor users, the developers, researchers, and founders who have made Tor possible are a diverse group of people. But all the people who have been involved in Tor are united by a common belief: internet users should have private access to an uncensored web.

(Continued on page 6)

(Continued from page 5)

https://www.torproject.org/ **Contact**: Email withheld by request.

Short Subject: Speaker: Mr. Art 'Coop' Cooper. **Topic:** Keeping Systems Patched: Why it is important and Why Nobody Seems to Get It Right. Contact: Mr. Cooper can be reached at artcoo1961@gmail.com.

August

6. 6 August 2020: **Speaker:** Mr. Michael Wylie, MBA, CISSP. Director of Cybersecurity Services, Richey May Technology Solutions. **Topic:** Introduction to Malware Analysis & Response (MA&R). **Synopsis:** IT and Cybersecurity professionals learned the basic workflow and techniques to safely analyze the characteristics/behavior of malware. Attendees received practical techniques and methodologies that can be immediately applied to statically and dynamically analyzing software with an emphasis on malicious software. **Contact:** Mr. Wylie can be reached at michael@richeymay.com.

7. 20 August 2020: **Speaker:** Mr. Vinnie Persichetti, Director of Cybersecurity Programs at Colorado Springs Chamber of Commerce & EDC. **Topic:** Cybersecurity in Colorado Springs. **Synopsis:** Update on Chamber & EDC grant-related efforts focused on the "Defense Diversification Program" and developing a marketing and branding strategy for the Colorado Springs cybersecurity ecosystem. **Contact:** Mr. Persichetti can be reached at VPersichetti@cscedc.com.

Speaker: Mr. Trent Bunnell Security +, Information Systems Security Officer, LinQuest**. Topic:** Encryption and Hashes. **Synopsis:** The story of execution, war, and over-reach. **Contact:** Mr. Bunnell can be reached at trent.b.bunnell@gmail.com.

September

8. 3 September 2020: **Speaker: T**erry Bradley, President, Mile High Cyber. **Topic:** Being a Virtual CISO. **Synopsis:** The difference between a fulltime and virtual CISO, various styles of CISOs, core jobs a CISO needs to handle, and lessons learned. **Contacts:** Mr. Bradley can be reached at terry.bradley@milehighcyber.com.

Short Subject: Speaker: Derick Lopez. **Topic:** Certifications: What's Out There? **Contact:** Mr. Lopez can be reached at derickl@msn.com.

9. 24 September 2020: **Speaker:** Mr. Sean Callahan, IRES CISO Jacobs. **Topic:** Hardening the Human Vulnerability. **Synopsis:** Why people are the greatest vulnerability to security and some ways to help remediate that vulnerability. **Contact:** Mr. Callahan can be reached at sean.callahan@jacobs.com.

Biden Team Highlights Cybersecurity Focus With First Cabinet Picks

By Mariam Baksh, Next Gov, November 23, 2020

The Biden-Harris transition team has explicitly called out cybersecurity as a priority in naming the first six individuals it plans to appoint or nominate for key cabinet positions.

In a formal announcement planned for Tuesday, President-elect Joe Biden and Vice President-elect Kamala Harris intend to introduce Antony Blinken for secretary of State, Avril Haines for director of national intelligence, Jake Sullivan for national security advisor, Alejandro Mayorkas for secretary of Homeland Security, Linda Thomas-Greenfield for U.S. ambassador to the United Nations and John Kerry as special presidential envoy for climate.

"These officials will start working immediately to rebuild our institutions, renew and reimagine American leadership to keep Americans safe at home and abroad, and address the defining challenges of our time—from infectious disease, to terrorism, nuclear proliferation, cyber threats, and climate change," reads a release Monday from the Biden transition team.

Mayorkas, Haines, Sullivan and Blinken will serve in roles crucial to cybersecurity policy and have all worked in the Obama administration, which pioneered enduring cybersecurity approaches centered on the development of public-private and international partnerships.

Mayorkas, who would be the new leader of DHS, was deputy secretary of the department during the Obama-Biden Administration from 2013 to 2016 and the challenges he confronted then around information sharing with the private sector are still front and center now. He's also tackled cybercrime and securities fraud as a U.S. attorney.

House Homeland Security Committee Chairman Bennie Thompson, D-Miss., praised Biden's selection of Mayorkas, noting his experience in cybersecurity.

"At a very nascent stage, the industry, individuals, companies ask of us, 'What is really in it for us? What is the benefit for us to share information?'" Mayorkas said in a 2016 speech in Israel. He invited that country to participate in the new information-sharing architecture that was being developed to help quickly disseminate indicators of compromise while protecting the private sector from fear of enforcement from their regulatory agencies and other legal liabilities.

But year after year, DHS' inspector general has highlighted a problematic lack of participation in the information-sharing mechanism by the private sector.

Read the rest here:

https://www.nextgov.com/cybersecurity/2020/11/biden-team-highlights-cybersecurity-focus-first-cabinet-picks/170274/

Rules for strong passwords don't work, researchers find. Here's what does

In the name of cybersecurity, you can stop adding an exclamation mark to the end of your password.

By Laura Hautala, Cnet, November 12, 2020

When you create a password for yet another new account, you'll probably encounter familiar rules designed to make it harder for hackers to get in: Use capital letters, numbers and special characters. These requirements, however, don't make your password stronger, researchers at Carnegie Mellon University say.

Lorrie Cranor, director of the CyLab Usable Security and Privacy Laboratory at CMU, says her team has a better way, a meter that websites can use to prompt you to create more-secure passwords. After a user has created a password of at least 10 characters, the meter will start giving suggestions, such as breaking up common words with slashes or random letters, to make your password stronger.

The suggestions set the password strength meter apart from other meters that provide an estimated password strength, often using colors. The suggestions come from common pitfalls Cranor's team has seen people make when they set up passwords during experiments run by the lab.

One of the problems with many passwords is that they tick all the security checks but are still easy to guess because most of us follow the same patterns, the lab found. Numbers? You'll likely add a "1" at the end. Capital letters? You'll probably make it the first one in the password. And special characters? Frequently exclamation marks.

CMU's password meter will offer advice for strengthening a password like "ILoveYou2!" -- which meets the standard requirements. The meter also offers other advice based on what you type in, such as reminding you not to use a name or suggesting you put special characters in the middle of your password.

"It's relevant to what you're doing, rather than some random tip," Cranor said.

In an experiment, users created passwords on a system that simply required them to enter 10 characters. Then the system rated the passwords with the lab's password strength meter and gave tailored suggestions for stronger passwords. Test subjects were able to come up with secure passwords that they could recall up to five days later. It worked better than showing users preset lists of rules or simply banning known bad passwords (I'm looking at you "StarWars").

Cranor and co-authors Joshua Tan, Lujo Bauer and Nicolas Christin will present their latest password findings on Thursday at the ACM Conference on Computer and Communications Security, which is being held virtually. The team hopes its tools will be adopted by website makers in the future.

Read the rest here:

https://www.cnet.com/news/rules-for-strong-passwords-dont-work-researchers-find-heres-what-does/

ISSA-COS 2021 Schedule of Events

Monthly Events

Chapter Meetings (6:00 – 7:30 PM) [1]

Tuesday, January 19, 2021 [2]
Tuesday, February 16, 2021 [2]
March – Quarterly/Annual Events
Tuesday, April 20, 2021 [3]
Tuesday, May 18, 2021 [3]
June – Quarterly/Annual Events
Tuesday, July 20, 2021 [3]
Tuesday, August 17, 2021 [3]
September – Quarterly/Annual Events
Tuesday, October 19, 2021 [3]
Tuesday, November 16, 2021 [3]
December – Quarterly/Annual Events

[1] Light Dinner Provided @ 5:30 PM
[2] Virtual Meeting; Recorded Playback Available
[3] In-person Meeting; Recorded Playback Available

Mini – Seminars (9:00 – 12:00 PM) [1]

Saturday, January 23, 2021 [2]
Saturday, February 20, 2021 [2]
March – Quarterly/Annual Events
Saturday, April 24, 2021 [3]
Saturday, May 22, 2021 [3]
June – Quarterly/Annual Events
Saturday, July 24, 2021 [3]
Saturday, August 21, 2021 [3]
September – Quarterly/Annual Events
Saturday, October 23, 2021 [3]
Saturday, November 13, 2021 [3]
December – Quarterly/Annual Events

[1] Continental Breakfast Provided @ 8:30 AM
[2] Virtual Meeting; Recorded Playback Available
[3] In-person Meeting; Recorded Playback Available

Quarterly Events

Virtual Security + CE Reviews

Saturday, March 6, 2021
Saturday, March 13, 2021
Saturday, March 20, 2021
Saturday, September 11, 2021
Saturday, September 18, 2021
Saturday, September 25, 2021

Virtual CISSP Review

Saturday, June 5, 2021
Friday, June 11, 2021
Saturday, June 12, 2021
Saturday, June 19, 2021
Friday, June 25, 2021
Saturday, June 26, 2021

Cyber Focus Symposium (CFS)

March 2021
CFS Girl Scout Cyber Camp

March 23 – 25, 2021
CFS Job Fair
CFS Capture-the-Flag Challenge
CFS Conference

Peak Cyber Symposium (PCS)

September 2021
PCS Girl Scout Cyber Camp

September 14 – 16, 2021
PCS Job Fair
PCS Capture-the-Flag Challenge
PCS Conference

(Continued on page 9

Annual Events

[2] Annual President's Address	>>	Tuesday, January 5, 2021 (6:00 – 7:00 PM)
[3] Annual Cyber SIG Summit	>>	Friday, June 18, 2021 (1:00 – 5:00 PM)
[4] Annual Cyber Social	>>	Friday, June 18, 2021 (5:00 – 9:00 PM)
Annual Chapter Elections	>>	Oct – Nov 2021 (Details TBA)
[4] Annual STAR Awards	>>	Friday, December 3, 2021 (5:00 – 9:00 PM)

[2] Virtual Meeting; Recorded Playback Available | [3] In-person Meeting; Recorded Playback Available | [4] In-person Meeting Only

For additional information, contact **info@issa-cos.org** or visit **www.issa-cos.org**.

ISSA-COS 2020 Annual Chapter Celebration (ACC)

Keynote Speaker: Ms. Erin Miller

ISSA Information Systems Security Association Colorado Springs Chapter

ISSA-COS Online Series December 2020 – Session 2

Date: December 17, 2020, 2020, 6 – 7:30 PM

Keynote Speaker:

- **Ms. Erin Miller**, Vice President of Operations, Space ISAC, NCC
- **Title: Space ISAC – An Overview of 2020 and a Preview of 2021**
- **Synopsis:** The Space ISAC serves to facilitate collaboration across the global space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to serve as the primary communications channel for the sector with respect to this information. Ms. Erin Miller will provide ISSA-COS with an update of recent and future events associated with the Space ISAC.

ACC Speaker:

- **Mr. Ernest Campos**, President, ISSA-COS
- **Synopsis:** The Annual Chapter Celebration (ACC) is a time for our chapter to celebrate the many accomplishments for our members, our chapter, and our community. During this event, ISSA-COS will honor our many volunteers, guest speakers, sponsors, strategic partners, and community partners for all they have done with and for our chapter in 2020.

Register at: www.issa-cos.org

Advanced Persistent Threat Actors Targeting U.S. Think Tanks

Original release date: December 01, 2020

Summary

This Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have observed persistent continued cyber intrusions by advanced persistent threat (APT) actors targeting U.S. think tanks. This malicious activity is often, but not exclusively, directed at individuals and organizations that focus on international affairs or national security policy.[1] The following guidance may assist U.S. think tanks in developing network defense procedures to prevent or rapidly detect these attacks.

APT actors have relied on multiple avenues for initial access. These have included low-effort capabilities such as spearphishing emails and third-party message services directed at both corporate and personal accounts, as well as exploiting vulnerable web-facing devices and remote connection capabilities. Increased telework during the COVID-19 pandemic has expanded workforce reliance on remote connectivity, affording malicious actors more opportunities to exploit those connections and to blend in with increased traffic. Attackers may leverage virtual private networks (VPNs) and other remote work tools to gain initial access or persistence on a victim's network. When successful, these low-effort, high-reward approaches allow threat actors to steal sensitive information, acquire user credentials, and gain persistent access to victim networks.

Given the importance that think tanks can have in shaping U.S. policy, CISA and FBI urge individuals and organizations in the international affairs and national security sectors to immediately adopt a heightened state of awareness and implement the critical steps listed in the Mitigations section of this Advisory.

Click here for a PDF version of this report.

Peak FBI: Hackers stole source code from US government agencies and private companies

By Catalin Cimpanu, ZDNet, November 7, 2020

The Federal Bureau of Investigation has sent out a security alert warning that threat actors are abusing misconfigured SonarQube applications to access and steal source code repositories from US government agencies and private businesses.

Intrusions have taken place since at least April 2020, the FBI said in an alert sent out last month and made public this week on its website.

The alert specifically warns owners of SonarQube, a web-based application that companies integrate into their software build chains to test source code and discover security flaws before rolling out code and applications into production environments.

SonarQube apps are installed on web servers and connected to source code hosting systems like BitBucket, GitHub, or GitLab accounts, or Azure DevOps systems.

But the FBI says that some companies have left these systems unprotected, running on their default configuration (on port 9000) with default admin credentials (admin/admin).

FBI officials say that threat actors have abused these misconfigurations to access SonarQube instances, pivot to the connected source code repositories, and then access and steal proprietary or private/sensitive applications.

Officials provided two examples of past incidents:

"In August 2020, unknown threat actors leaked internal data from two organizations through a public lifecycle repository tool. The stolen data was sourced from SonarQube instances that used default port settings and admin credentials running on the affected organizations' networks.

"This activity is similar toa previous data leak in July 2020, in which an identified cyber actor exfiltrated proprietary source code from enterprises throughpoorly secured SonarQube instances and published the exfiltrated source codeon a self-hosted public repository."

FORGOT PROBLEM RESURFACES IN 2020

The FBI alert touches on a little known issue among software developers and security researchers.

While the cyber-security industry has often warned about the dangers of leaving MongoDB or Elasticsearch databases exposed online without passwords, SonarQube has slipped through the cracks.

However, some security researchers have been warning about the dangers of leaving SonarQube applications exposed online with default credentials since as far back as May 2018.

At the time, data breach hunter Bob Diachenko warned that about 30% to 40% of all the ~3,000 SonarQube instances available online at the time had no password or authentication mechanism enabled.

This year, a Swiss security researcher named Till Kottmann has also raised the same issue of misconfigured SonarQube instances. Throughout the year, Kottmann has gathered source code from tens of tech companies in a public portal, and many of these came from SonarQube applications.

"Most people seem to change absolutely none of the settings, which are actually properly explained in the setup guide from SonarQube," Kottmann told *ZDNet*.

"I don't know the current number of exposed SonarQube instances, but I doubt it changed much. I would guess it's still far over 1,000 servers (that are indexed by Shodan) which are 'vulnerable' by either requiring no auth or leaving default creds," he said.

Read the rest here:

https://www.zdnet.com/article/fbi-hackers-stole-source-code-from-us-government-agencies-and-private-companies/?fbclid=IwAR0Qhgo6EZWXj6kTA9nPYmHgBG_yl_ixNUcWBufujHv0ztOtA8Xt5jBcGvo

Making Sure Virtual Doctor Visits Are Private and Secure

By Jennifer Cawtha, NIST, October 21, 2020

"Telehealth" refers to a wide range of technologies to connect patients to health care services through videoconferencing, remote monitoring, electronic consultations and wireless communications. Just like you would expect your virtual conversation with your doctor to be private and secure, you would also want to be sure that all your other health information that is transmitted over the internet or cellular networks is also protected.

In October 2018, the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) launched a project focusing on the cybersecurity and privacy challenges surrounding monitoring the health of patients remotely via telehealth. When we started the project, telehealth was for the most part only available to patients in rural areas or in a health care setting, but has since exploded to become more accessible.

Who knew then that in 18 months even more patients — under stay-at-home orders and eager to avoid being exposed to the coronavirus — would choose telehealth over traditional doctor visits? In addition to being a safer option during a pandemic by allowing patient and clinician to maintain a safe distance from each other, telehealth allows the patient to remain in the comfort of their home during recovery or monitoring. It also can provide better access to health care for patients, ease access to patient data and allow the clinician to deliver higher-quality care to more patients.

For this project, my team and I are focused on remote patient monitoring (RPM). RPM is a convenient and cost-effective service for patients who have health conditions that require regular clinician monitoring, and typically where in-person visitation is impractical. Clinicians use sensors connected to internet-based technologies to track the patient's vital signs (e.g., blood pressure, heart rate, weight, glucose levels, etc.) while the patient remains in their home.

As the growth and popularity of telehealth increases, it is critical to evaluate the security and privacy risks. We are working closely with the NIST privacy team to ensure we capture a complete picture of the risks. Once identified, we implement security controls such as encryption to minimize the security and privacy risks to the patients and other participants.

We augmented our NCCoE team with private industry collaborators representing technology vendors, health care cybersecurity experts and health systems representatives. Our collaborators responded to a call in the *Federal Register*. Companies with relevant products and expertise were invited to participate in a consortium to build an example solution that improves the security and privacy for the wide range of devices and systems used to facilitate communication between the patient and the health care provider.

With our team finalized in early March, we were off to a great start.

That was short-lived, however, as everything soon changed due to the COVID-19 pandemic. We no longer had physical access to our lab, and gone were the days when we could jointly huddle over a laptop to collaboratively troubleshoot issues. Also gone were the impromptu discussions over coffee. Instead, we could only have online meetings. Accepting our new situation, we quickly pivoted to using a variety of collaboration tools to work with our industry team members to remotely install, configure and integrate their technologies to build an example solution. We are currently finalizing it and will test it to ensure it addresses the cybersecurity and privacy challenges.

Fortunately, this new reality hasn't really slowed down our team's work.

In assessing the RPM ecosystem, we identified three primary domains: the health delivery organization (HDO), the telehealth provider, and the patient home. Because each domain is managed and used by different people or organizations with different skill levels, the risks of accidental security misconfigurations and other threats may manifest differently. The patient, however, is the primary actor in the RPM scenario as they are the ones hooking themselves up to the various monitoring devices and using the systems that communicate with care providers.

Read the rest here:

https://www.nist.gov/blogs/taking-measure/making-sure-virtual-doctor-visits-are-private-and-secure

Join ISSA-COS on 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/

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**

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

Vietnam-Linked Cyberspies Use New macOS Backdoor in Attacks

By Ionut Arghire, Security Week, November 30, 2020

Trend Micro's security researchers have identified a new macOS backdoor that they believe is used by the Vietnamese threat actor OceanLotus.

Also referred to as APT-C-00 and APT32, and believed to be well-resourced and determined, OceanLotus has been observed mainly targeting government and corporate entities in Southeast Asia. Earlier this year, the group engaged in COVID -19 espionage attacks targeting China.

Compared to previous malware variants associated with OceanLotus, the newly discovered sample shows similarities in dynamic behavior and code, clearly suggesting a link to the threat actor.

A document used in the campaign features a Vietnamese name, which has led researchers to believe that users from Vietnam have been targeted with the new malware.

The observed sample masquerades as a Word document but it is an app bundled in a ZIP archive, which features special characters in its name, in an attempt to evade detection.

The app bundle, Trend Micro explains, is seen by the operating system as an unsupported directory type, meaning that the 'open' command is used to execute it.

Within the app bundle, the security researchers discovered two files, namely a shell script that performs multiple malicious routines, and a Word file that is displayed during execution.

The shell script is responsible for deleting the file quarantine attribute for the files in the bundle and for removing the file quarantine attribute of files in the system, copying the Word document to a temp directory and opening it, extracting the second -stage binary and changing its access permissions, then deleting the malware app bundle and the Word document from the system.

Read the rest here:

https://www.securityweek.com/vietnam-linked-cyberspies-use-new-macos-backdoor-attacks

Cybersecurity Predictions for 2021: Robot Overlords No, Connected Car Hacks Yes

By Saryu Nayyar, Threat Post, November 27, 2020

Predicting the future is always an iffy proposition. There's the Nostradamus route, making predictions so cryptic and vague they could mean just about anything. Or you can go the TV psychic route and throw a handful of darts at the wall, highlighting the ones that stick and hope everyone ignores the many misses.

In cybersecurity, the best we can do is look at trends in attack methodologies, recognize changes in the threatscape, see what new technologies are emerging and offer a best guess about where things will be going forward.

We will get it wrong part of the time. Possibly most of the time. But we are coming at it from the angle of cybersecurity professionals familiar with where we were and where we are, and with some insight into where we're going. Let's hope we can do better than celebrity psychics who never seem to have the foresight to make a mint by picking the next big stock.

With that in mind, here are some predictions about the world of cybersecurity going into 2021. While 2020 makes us inclined to predict that "quantum computing will make machines sentient and the robots will rise up and kill us all," the future does not look *that* bad.

Ransomware Will Evolve

Cyberattacks have matured over the years, with different trends coming and going. Going into 2021, ransomware will almost certainly remain a big part of the attacker's portfolio, but cybercriminals will continue to "add value" by also stealing data before they encrypt it. We have seen them use this added extortion tactic already, but this will become more of an issue in the healthcare space, where attackers can use stolen patient records to blackmail patients by threatening to release medical histories.

Sadly, continued attacks against healthcare and medical infrastructure will probably lead to serious consequences going into 2021. Someone will likely die as the direct result of a cyberattack. The only positive outcomes here are that the tragic wakeup call will be the impetus needed to beef up defenses in the healthcare space and make law enforcement more aggressive pursuing cybercriminals.

As cybercriminals continue to evolve their business models, they will become bolder and target a broader range of industries. They will still go after targets of opportunity as low-hanging fruit, but expect to see more targeted attacks against companies, and industries, that had not previously considered themselves at high risk. This includes any organization outside the top five: Financial services, government, healthcare, higher education or the energy sector.

Zero-Days and Cryptocurrency

Zero-day attacks against popular operating systems and applications will continue to be an issue too. Developers have become more careful overall, but there is still room for improvement. Bug bounties help (offered by major vendors for people to improve their code), but malicious actors will continue to use their version of the same model and offer high payouts to people who sell them exploits.

Cryptocurrency remains a volatile pseudo-commodity that is favored by privacy advocates and criminals, while it is loathed by government agencies. From the perspective of cybersecurity, cryptominers have become a common payload for attackers simply going after compute resources. We are likely to see more of them going forward.

Governments are already working to regulate the space and 2021 may see legislation seeking to control, if not outright ban, the use of cryptocurrencies. Law-enforcement agencies worldwide will need to cooperate if they are to have any chance of dealing with an ever-growing cybercriminal underground. The criminals' evolving business models may actually make them easier to target by law enforcement.

The IoT Tsunami – and Connected Cars

Internet of things (IoT) devices will continue to live largely unseen and unnoticed as they're compromised. Separate from the larger devices such as medical imaging systems, small IoT devices will remain vulnerable and unpatched, if not unpatchable, as they become ubiquitous. Malicious actors will find new and more creative uses for these devices, possibly finding ways to use them to compromise the cloud-based controllers they frequently rely on.

Read the rest here:

https://threatpost.com/cybersecurity-predictions-2021-robot-overlords-connected-car/161594/

Army launches 'Hack the Army 3.0' with more targets for cybersecurity researchers

By Jackson Barnett, FedScoop, November 9, 2020

The Army is launching a third edition of its "Hack the Army" bug bounty program, with a plan for increasing participation in the program and offering more targets to hack.

Hack the Army 3.0 is set to start Dec. 14 and run until Jan. 28, or until all funding has been doled out to winners. The Army didn't specify how much money is available. Hack the Army 2.0 awarded $275,000 in late 2019.

The entire Army.mil domain can be targeted this time by participating white-hat hackers, but the Army said it will only pay for discoveries in certain categories of vulnerabilities. Other available targets include sign-on/authentication services and Army-owned VPNs.

The program, run in partnership with Defense Digital Services, Army Cyber Command and the company HackerOne, mirrors other bug bounty programs across the military. The Department of Defense has tried to expand bug bounty programs as a means to catch security vulnerabilities, with the Air Force going as far as wanting hackers to be able to "make a living" off their bug bounty programs.

"The bounties offer both military and civilian participants a unique way to serve their country, while providing an innovative and effective means of 'crowdsourcing' security solutions more quickly and economically than by developing similar solutions through more traditional methods," the Army said in its release.

Read the rest here:

https://www.fedscoop.com/hack-the-army-3-hackerone/

Navy invention powers wireless devices through vibrations, walking

By Staff, TechLink, Undated

A new U.S. Navy invention hopes to be the engine inside a portable generator, enabling wireless devices to be powered by walking, driving, or even playing music.

The invention is the brainchild of Adi Bulsara from the Naval Information Warfare Center in San Diego, as well as a team of scientists from Italy.

On July 28, 2020, the Navy was granted U.S. Patent 10,727,394 for their work, which included a prototype and testing.

The invention uses an ultra-flexible polyethylene terephthalate (PET) beam in a snap-through-buckling (STB) configuration and a magnetic repulsion mechanism in order to harness vibrations and turn them into mechanical energy.

With it, low-frequency vibration sources, like walking and running, vehicles, or handheld tools, could power wireless devices.

There have been similar efforts made in the past, but the complexities and low efficiencies made those devices impractical.

However, the non-linear nature of the Navy invention provides higher rates of return with a simpler mechanism. It also allows for a broader frequency of vibrational activities to be harvested.

"The exploitation of new harvesting configurations based on non-linear mechanisms, such as bi-stable systems, has the potential to outperform traditional (linear) energy harvesters under the right set of operating conditions," according to the patent.

The new technology is available to companies via license agreement who would commercialize it. TechLink is the Department of Defense's national partnership intermediary for technology transfer. Located at Montana State University, the organization provides licensing services to businesses at no cost.

Read the rest here:

https://techlinkcenter.org/news/navy-invention-powers-wireless-devices-through-vibrations-walking

This hacking group is using previously unknown tools to target defence contractors

By Danny Palmer, ZDNet, November 6, 2020

Hackers used previously unknown tools in a cyber-espionage campaign targeting defence and aerospace companies in a social engineering and phishing campaign that is more widely targeted than first thought.

Researchers at McAfee first detailed Operation North Star earlier this year, but further analysis reveals additional tactics and techniques of the campaign that has almost identical elements to Hidden Cobra – AKA The Lazarus Group – a hacking operation which the US government and others say is working out of North Korea on behalf of the government in Pyongyang.

The campaign is still based around spear-phishing emails and LinkedIn messages that pose as job recruitment messages in an effort to lure victims into opening malicious attachments. Hackers even use legitimate recruitment adverts and documents taken from popular US defence contractor websites to make the emails look more authentic.

But now additional analysis by McAfee has revealed how the attackers use two stages of malware implants. All targets are compromised with the first stage of malware, which allows attackers to gather data including disk information, free disk space, computer name and logged-in username and process information.

The hackers analyse this information to determine if the victim is of high enough value to continue to with an attack – if the victim isn't deemed important enough, the machine is sidelined while the attackers focus on distributing a second stage malware to victims deemed more worthwhile of attention.

The second stage uses a previously known implant called Torisma, a custom-developed tool focused on specialised monitoring of high-value victims' systems, looking to gain access to login credentials and remote desktop sessions – all while remaining undetected.

"What is clear is that the campaign's objective was to establish a long-term, persistent espionage campaign focused on specific individuals in possession of strategically valuable technology from key countries around the world," McAfee researchers said in a blog post.

For Operation North Star, this meant researching specific target victims and creating custom content to lure victims in, then infecting them with malware in an effort to commit espionage.

Initial reporting of the campaign detailed attacks against targets in the US, but those weren't the only ones hackers were looking to compromise – analysis of the attacks has revealed that defence and technology contractors in Israel, Russia, India and Australia have also been targeted by this campaign.

"The actors behind the campaign were more sophisticated than they initially appeared. They are focused and deliberate in what they meant to achieve and more disciplined and patient in executing to achieve their objective," said researchers.

Read the rest here:

https://www.zdnet.com/article/this-hacking-group-is-using-previously-unknown-tools-to-target-defence-contractors/

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: Steven Mulig
- Deputy: **Vacant**

Vice President of Training: Mark Heinrich
- Deputy: Phebe Swope

Member at Large: Art Cooper
Member at Large: Jim Blake
Member at Large: James Asimah
Member at Large: Dennis Kater

Committee Chairs:

Training: Mark Heinrich
Mentorship Committee Chair: **Vacant**
Media/Newsletter: Don Creamer
IT Committee: Patrick Sheehan
Speaker's Bureau: William (Jay) Carson

**** 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

Extraordinary Vulnerabilities Discovered in TCL Android TVs, Now World's 3rd Largest TV Manufacturer

By Admin, Sick.Codes, November 9, 2020

The following piece is the culmination of a three-month long investigation into Smart TVs running Android. Having lived through this research experience, I can wholeheartedly say that there were multiple moments that I, and another security researcher that I met along the way, couldn't believe what was happening. On multiple occasions I found myself feeling as though, "you couldn't even make this up…"

I'm a security researcher, a freelance developer, and a hacker.

Read the rest here:

https://sick.codes/extraordinary-vulnerabilities-discovered-in-tcl-android-tvs-now-worlds-3rd-largest-tv-manufacturer/

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