WWW.ISSA-COS.ORG

ISSA-COS NEWSLETTER

VOLUME 8 NUMBER 6 JUNE 2019

Colorado Springs, Colorado

A Great Honor for Our Chapter

ISSA-COS Members,

In addition to our regular programming, the month of May privileged our chapter to an incredible honor. We were contacted by the U.S. State Department via our local COS Chamber and EDC with a request to host a round table discussion for a delegation of Cybersecurity professionals from Mongolia. The delegation was a mixture of government officials, military commanders, and public sector professionals. Officials within Mongolia have implemented foundational Cybersecurity capabilities and are now seeking advice from businesses and organizations in the United States on how best to institute policies and procedures to govern their current capabilities. They were also seeking advice on topics such as cyber hygiene, public security awareness, and physical and logical cybersecurity protection. Colorado Springs was their third stop on a five-city tour which includes Washington DC, Pittsburgh, Colorado Springs, San Francisco, and Honolulu.

The round table event was held in the Executive Board Room of the Wells Fargo Tower in downtown Colorado Springs. In addition to organizing the event, ISSA-COS drafted discussion topics/questions from a list of provided objectives and staffed a panel of Cybersecurity professionals from small, medium, and large businesses within our region. The panel members from ISSA-COS that participated in this event included:

Steven Mulig – Government Cybersecurity Solutions
Darla Lindt – Risk Mitigation and Insurance
Eric Bailey – Cybersecurity Architect and Engineering
Jerry Chappee – Global Cybersecurity Solutions
Ernest Campos (Moderator) – Cybersecurity Leadership and Innovation

Just two days following this event, we received feedback from the delegation (now in San Francisco) that they considered their time spent with ISSA-COS to be the most beneficial time on their entire tour. So much so, they want to initiate an ISSA chapter within Mongolia to establish a program of knowledge growth, social education, and industry advancement. What an honor for our chapter to have had the opportunity to affect not only our industry but, an entire nation. **Good job ISSA-COS!** This event really demonstrated the strength and value

(Continued on page 4)

A Note From Our President

By Mr. Ernest Campos

How Chinese Spies Got the N.S.A.'s Hacking Tools, and Used Them for Attacks

By Nicole Perlroth, David E. Sanger and Scott Shane, New York Times, May 6, 2019

On May 7, hackers infected about 10,000 of Baltimore city government's computers with an aggressive form of ransomware called RobbinHood, and insisted the city pay 13 bitcoin (then $76,280, today $102,310) to cut the computers loose. The hackers claimed the price would go up every day after four days, and after the tenth day, the affected files would be lost forever.

Chinese intelligence agents acquired National Security Agency hacking tools and repurposed them in 2016 to attack American allies and private companies in Europe and Asia, a leading cybersecurity firm has discovered. The episode is the latest evidence that the United States has lost control of key parts of its cybersecurity arsenal.

"One attack on a major telecommunications network may have given Chinese intelligence officers access to hundreds of thousands or millions of private communications ..."

Based on the timing of the attacks and clues in the computer code, researchers with the firm Symantec believe the Chinese did not steal the code but captured it from an N.S.A. attack on their own computers — like a gunslinger who grabs an enemy's rifle and starts blasting away.

The Chinese action shows how proliferating cyberconflict is creating a digital wild West with few rules or certainties, and how difficult it is for the United States to keep track of the malware it uses to break into foreign networks and attack adversaries' infrastructure.

The losses have touched off a debate within the intelligence community over whether the United States should continue to develop some of the world's most high-tech, stealthy cyberweapons if it is unable to keep them under lock and key.

The Chinese hacking group that co-opted the N.S.A.'s tools is considered by the agency's analysts to be among the most dangerous Chinese contractors it tracks, according to a classified agency memo reviewed by The New York Times. The group is responsible for numerous attacks on some of the most sensitive defense targets inside the United States, including space, satellite and nuclear propulsion technology makers.

Now, Symantec's discovery, unveiled on Monday, suggests that the same Chinese hackers the agency has trailed for more than a decade have turned the tables on the agency.

Some of the same N.S.A. hacking tools acquired by the Chinese were later dumped on the internet by a still-unidentified group that calls itself the Shadow Brokers and used by Russia and North Korea in devastating global attacks, although there appears to be no connection between China's acquisition of the American cyberweapons and the Shadow Brokers' later revelations.

But Symantec's discovery provides the first evidence that Chinese state-sponsored hackers acquired some of the tools months before the Shadow Brokers first appeared on the internet in August 2016.

Repeatedly over the past decade, American intelligence agencies have had their hacking tools and details about highly classified cybersecurity programs resurface in the hands of other nations or criminal groups.

The N.S.A. used sophisticated malware to destroy Iran's nuclear centrifuges — and then saw the same code proliferate around the world, doing damage to random targets, including American business giants like Chevron. Details of secret American cybersecurity programs were disclosed to journalists by Edward J. Snowden, a former N.S.A. contractor now living in exile in Moscow. A collection of C.I.A. cyberweapons, allegedly leaked by an insider, was posted on WikiLeaks.

"We've learned that you cannot guarantee your tools will not get leaked and used against you and your allies," said Eric Chien, a security director at Symantec.

Now that nation-state cyberweapons have been leaked, hacked and repurposed by American adversaries, Mr. Chien added, it is high time that nation states "bake that into" their analysis of the risk of using cyberweapons — and the very real possibility they will be reassembled and shot back at the United States or its allies.

Read the rest here:

https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html?emc=edit_th_190507&nl=todaysheadlines&nlid=10437390507

Membership Corner

Membership Update

The deadline for 2019 Fellows cycle submissions is June 17, 2019! The Fellows Program formally recognizes significant contributions to the cyber community, cyber profession, ISSA leadership and sustained ISSA membership. The elite status of Distinguished Fellow designation is limited to only 1% of ISSA members and Fellow status is limited to 2% of the ISSA membership. Senior Membership is also an option. Information about the requirements and how to apply can be found on the ISSA International website at https://www.issa.org/page/FellowProgram. See page 8 in this newsletter.

If, after reviewing the requirements for Distinguished Fellow, Fellow or Senior Member, you believe you meet the criteria and are interested in submitting a package please contact Dave Reed at membership@issa-cos.org or any board member at cos-board-new@issa-cos.org.

New Members May
Nigel Webb
Larry Langston
James Stewart
Monica Tauscher-Baker
Richard LaCroix
Brian Osterhaus
Eric Harashevsky
Mamoun Hajjar
Bill Clark III
Michael Reddick

Our membership is holding at ~460 members as of the end of May. I would also like to welcome our new members on behalf of the Chapter! When you're participating in Chapter activities, please take a moment to introduce yourself to members of the board, me, and other members. Don't forget to identify yourself as a new member and feel free to ask for help or information. Thanks for joining the Chapter and don't forget to look for opportunities to lend your expertise to improve the Chapter. We're always open to new ideas and suggestions.

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,

David Reed

Membership Committee Chairman

membership@issa-cos.org

Former U.S. Secretary of State Hillary Rodham Clinton to Keynote FireEye Cyber Defense Summit

By Staff, Business Wire, May 30, 2019

FireEye, Inc., the intelligence-led security company, today announced details for FireEye Cyber Defense Summit 2019, taking place October 7-10 at the Washington Hilton in Washington, D.C.

Among the keynote speaker lineup, Former U.S. Secretary of State Hillary Rodham Clinton will engage in a Q&A discussion with FireEye CEO, Kevin Mandia on the geopolitical landscape and its implications for global cyber security today. Secretary Clinton has been a practicing attorney and law professor, an advocate of internet freedom, First Lady, and U.S. Senator from New York, in addition to serving as the 67th United States Secretary of State.

Read the rest here:

https://www.businesswire.com/news/home/20190530005027/en/U.S.-Secretary-State-Hillary-Rodham-Clinton-Keynote

 (Continued from page 1)

we provide to our industry ecosystem.

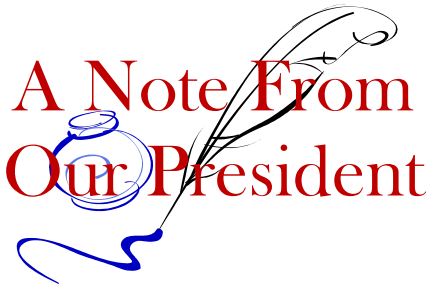
Well, if that wasn't enough, ISSA-COS is also gearing up for our Q2 Special Interest Group (SIG) Gathering. This event will be held on Thursday, June 20th from 6 – 8 PM at the Pikes Peak Community College (PPCC) Centennial Campus. This event will feature the following eight (8) SIGs; four (4) Affinity groups and four (4) Industry groups.

Affinity Groups

W*[omen]* in Security
Y*[oung Professionals]* in Security
E*[ducators]* in Security
E*[xecutives]* in Security

Industry Groups

H[ealthcare] in Security
R[etail] in Security
F[inance] in Security
D[od] in Security



Please, please, please help spread the word for this event! We are striving to continually increase participation among Information Technology and Cybersecurity professionals across **ALL** industries in our community. The schedule for this event will be as follows:

PPCC Centennial Campus Room #	Session 1: Affinity SIGs 6:00 – 6:45 PM	Networking Break 6:45 – 7:15 PM	Session 2: Industry SIGs 7:15 – 8:00 PM
PA 222	Women in Security (WIS)	Appetizers and drinks in the Atrium. Please bring and share business cards, resumes, and flyers for upcoming events.	Healthcare in Security (HIS)
PA 226	Young Professionals in Security (YIS)		Finance in Security (FIS)
PA 259	Educators in Security (EduIS)		Retail in Security (RIS)
PA 323	Executives in Security (EIS)		DoD in Security (DoDIS)

As was announced during our May Chapter Meetings, ISSA-COS is launching a "**Breakfast with ISSA-COS**" industry outreach. Nominate your company and if chosen, ISSA-COS will arrange for Oliver's Deli to come into your company and sell breakfast burritos, bagel sandwiches, and sweet breads at a **15% discount**; compliments of ISSA-COS. In addition to breakfast, we will also have a chapter representative present to promote our chapter and provide information on membership and sponsorship opportunities. Breakfast with ISSA-COS will launch in July. If you are interested in having your company participate, contact us at info@issa-cos.org and we will add you to the schedule. If your company is selected, you will receive a **FREE** breakfast! Don't wait…. contact us **NOW**!

Last of all, it is time to gear up for our 2019 **Peak Cyber** conference being held September 3rd, 4th, and 5th at the DoubleTree Hotel. Registration for speakers and sponsors has already opened (https://www.fbcinc.com/event.aspx/Q6UJ9A019PGH#speakers) and registration for attendees will soon open. When it does, please register early and often! Early registration strengthens our ability to secure the best guest speakers available. The theme for this year's Peak Cyber conference is: "**Cyber Hygiene: Everyday for Everyone**." This year, we are seeking to represent as many industries as possible while supporting the emphasis of our theme.

In closing, our Board of Directors wants everyone to understand how much we appreciate our general members. The strength of our organization resides in the size, knowledge, and diversity of our membership. Without all of you, across our region, doing what you do every day, we would not be the institution that we are. Our community looks towards ISSA-COS for Cybersecurity truth, vision, and direction. It is because of you, all of you, that we are who we are. Thank you for your support. Please consider volunteering for our current board and key personnel openings. Consider joining our Volunteer Corps distribution list to attend community events on behalf of our chapter. And, at your next healthcare, financial, or retail experience, consider inviting the IT or Cyber professional from those organizations to our next SIG gathering or Peak Cyber conference. Among our nearly 500 members, five minutes of your time to invite someone else could make a huge difference for our chapter.

As always, thank you for your support, participation, and membership.

Sincerely,

Ernest

Call for Articles: "Best of ISSA-COS" 2019

- Network and Infrastructure Security
- Web Security
- Endpoint Security
- Application Security
- Managed Security Service Providers
- Data Security
- Mobile Security
- Risk and Compliance
- Identity and Access Management
- Security Operations and Incident Response
- Threat Intelligence
- IoT
- Messaging Security
- Digital Rights Management
- Security Consulting
- Blockchain
- Fraud and Transaction Security
- Cloud Security

Deadline: August 16, 2019

Breakfast with ISSA-COS

ISSA-COS will arrange for Oliver's Deli to come sell breakfast at your office!

Patrons will receive a **15% discount** on all food items… *compliments of ISSA-COS!*

An ISSA-COS representative will be on hand to provide membership and sponsorship information.

Nominate your company and

YOU EAT FREE!

Meet the Board Member

As members of the Colorado Springs Chapter of the ISSA you get to enjoy a great number of benefits such as Monthly Meetings, Mini Seminars, Conferences and networking with peers. As a not-for-profit organization these things can only be accomplished thanks to the volunteers who make them happen. In this edition, we are going to highlight and get to know our chapter Professional Outreach Director, Katie Martin. Katie has the difficult task of connecting with outside interests and introducing them to the ISSA organization, specifically our chapter. Below are some questions I posed to her and her responses.

How long have you been a member of ISSA (COS)?

I first joined ISSA-COS in 2017 as a student member after learning about the organization through SecureSet Academy. In late 2018 I upgraded my membership to a General Member. This upgrade to my membership afforded me the opportunity to run for the position of Director of Professional Outreach to which I was elected and have immensely enjoyed not only the role, but also the vast opportunities to not only network with key cyber organizations and professionals but to also learn about all the activities and funding allotted towards growing the cybersecurity workforce in Colorado Springs.

Why did you decide to join the Board for ISSA-COS?

After learning about the many networking events and educational seminars hosted by ISSA, I decided this would be a rare and great opportunity to advocate for, and serve in, the local cybersecurity community. I also feel it's paramount to drive awareness of ISSA-COS and all the benefits it provides to its members.

Tell us something about yourself?

I'm an unapologetic American patriot through and through. I've spent much of the last 15 years of my personal life dedicated to learning as much as possible about World War II history. I believe it's important to not only 'never forget' but to also know one of the biggest battles in US history and how much our country sacrificed in protection of the liberties we have today.

What is your experience in the Information Systems Security arena?

My experience includes, basically, re-booting my career after early retirement (18 years) with Hewlett-Packard. I chose to go back to school in cybersecurity. I chose cybersecurity because of my innate curiosity of what "cybersecurity" means, the great need for cyber professionals and something that challenged me to learn a very dynamic and complex real-time battle America faces in the digital world. After attending school, I moved forward to study for CompTIA's Security+ certification (the hardest test I've ever conquered) in which I passed in July 2018.

Do you have one "horror" story about Cyber Security you can share?

I think my initial horror (or fear) was, in reading cybersecurity books on the origins of America's cyber defense, learning our country was miles behind Russia and Russia's active and advanced exploitations of America in cyber espionage. A large part of the cybersecurity movement in the federal government stemmed from, no kidding, President Ronald Reagan watching War Games and being so shaken by the thought it could actually happen, that the next day he called in his Joint Chiefs to see if it could really happen – to which they replied it absolutely could. Hence, Reagan signed in the first meaningful cyber defense Executive Order.

How has the Chapter helped/supported you?

There's really no beginning nor end to how the ISSA-COS has supported me. Not only did the Security+ seminars help prepare me to pass my certification, I opportunized on its networking events, and through those events, met the Talent Acquisition Manager for Boecore. Desperately in need of a job and security clearance, this connection was the pivot point in my career. I was selected as a candidate for an interview with Boecore and its prime, Booz Allen Hamilton (BAH). I was chosen for the position and am now going through security clearance to be a Cybersecurity Systems Analyst working with BAH on an Air Force satellite and GPS contract. As a space junkie, I couldn't be more "geeked out" and excited to start my new job.

How would you like to see the Chapter grow and/or expand?

The ISSA-COS chapter has afforded me so many opportunities I never knew existed. I am passionate about, and 100% invested in, evangelizing ISSA and driving awareness of the many benefits of being a member.

Mike Crandall

ISSA-COS Vice-President

Platinum Sponsor—Murray Security Services—
https://www.murraysecurityservices.com/

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Aero Sponsor—CT Cubed
https://www.ctcubed.com/

ISSA Nametags

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

Blue Ribbon Trophies & Awards
245 E Taylor St (behind Johnny's Navajo Hogan on North Nevada)
Colorado Springs
(719) 260-9911

Although their hours are officially Monday through Friday until 5:30 pm, they are occasionally in the shop on Saturdays. This is a small business so cash/check would be appreciated. Email wbusovsky@aol.com to order.

ISSA Fellow Program

2019 Fellows Cycle Now Open

The Colorado Springs ISSA Chapter has over 500 current members. Many of you have been members for several years and may qualify for the ISSA fellow program. The Fellow Program recognizes sustained membership and contributions to the profession. If you think you or another ISSA associate may qualify in the fellow program, please contact Jorden Smith at jordenbsmith96@gmail.com to coordinate the process. Erik is the chair of the chapter awards committee and will help you through the steps. Below are some details on the ISSA Fellow Program. Qualification information is also presented below:

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

Nominations and applications are accepted on an annual cycle. Applications will be accepted until **June 17, 2019 at 5:00pm Eastern Time**. Following the application period, there will be a ten week review period followed by the notification and presentation process. Fellows and Distinguished Fellows will be recognized at the 2018 ISSA International Conference.

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

To Become a Senior Member

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

Senior Member Qualifications

- 5 years of ISSA membership
- 10 years relevant professional experience
- For your convenience, please feel free to use this **Senior Member Application Check-list** to confirm eligibility and completion of application

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

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

To Become a Fellow or Distinguished Fellow

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

Fellow Qualifications

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

All Fellow applications require a nomination to qualify.

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

(Continued on page 9)

(Continued from page 8)

Distinguished Fellow Qualifications

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

All Distinguished Fellow applications require a nomination to qualify.

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

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

Jorden Smith
Recognition Committee Chair
jordenbsmith96@gmail.com

Volunteer Opportunities

Board Positions	Key Personnel	Volunteer Corps
Deputy Recorder/Historian **Deputy Treasurer** **Deputy VP of Training** **Member-at-Large**	**SIG Committee Chair** **Recognition Committee Chair** **SIG Leaders:** • ***Finance*** • ***Retail*** • ***Educators*** • ***Executives***	**Increase community awareness of our chapter** **Expand community involvement for our members** **Attend industry relevant events throughout Colorado** **Earn additional CPE/CPU credits** **Increase network connections**

2019 Schedule of Events

Chapter Meetings – Dinner

Tuesday, July 16, 2019
Tuesday, August 20, 2019
Tuesday, October 15, 2019
Tuesday, November 19, 2019

Chapter Meetings – Lunch

Wednesday, July 17, 2019
Wednesday, August 21, 2019
Wednesday, October 16, 2019
Wednesday, November 20, 2019

Mini-Seminars

Saturday, July 20, 2019
Saturday, August 24, 2019
Saturday, October 19, 2019
Saturday, November 23, 2019

Special Interest Group Gatherings

Thursday, June 20, 2019
Thursday, September 5, 2019
Thursday, December 5, 2019

ISSA-COS Conferences Peak Cyber

Tuesday, September 3, 2019
Wednesday, September 4, 2019
Thursday, September 5, 2019

Quarterly Recognition & Networking Events

Tuesday, June 18, 2019
Tuesday, September 3, 2019
Thursday, December 5, 2019

Security +CE Reviews

Saturday, September 14, 2019
Saturday, September 21, 2019
Saturday, September 28, 2019

CISSP Review

Friday, June 7, 2019
Saturday, June 8, 2019
Saturday, June 15, 2019
Friday, June 21, 2019
Saturday, June 22, 2019
Saturday, June 29, 2019

Annual Award Ceremony

Thursday, December 5, 2019

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

Space: Jack The Signal

By Staff, Strategy Page, May 29, 2019

Since 2015 Russia has been using eastern Ukraine and Syria for testing new EW (Electronic Warfare) equipment. New gear is tested "under combat conditions" to discover weaknesses and promote export sales as "combat proven". Equipment still in development is also tested. A recent example of that is the truck mounted Tirada-2 orbital jamming system that recently showed up in eastern Ukraine. Tirada-2 was seeking to hack the control signals and video feeds from American RQ-4B Global Hawk UAVs that regularly operate over eastern Ukraine. This would provide a look at what these UAVs see when they monitor Russian activity. Some RQ-4Bs are equipped with "space satellite quality" electronic sensors and the Russians are hoping to get an opportunity to monitor and perhaps hack those systems. Ukrainian and Western intelligence was aware of the existence of Tirada-2 if only because a less capable export model was being offered for sale. But now the more capable non-export Tirada-2 appears to have shown up in Eastern Ukraine (Donbas) but, as one would expect, no one is providing any details of who has been able to do what to whom.

Hacking and jamming satellites is nothing new. Even Islamic terrorists are active in this area. For example in early 2015 a major French TV network (TV5) was hijacked by hackers working for ISIL (Islamic State in Iraq and the Levant). Calling themselves the CyberCaliphate, this group had apparently spent weeks getting past the formidable network security and did some major damage. TV5 satellite feeds sends programming to over 250 million customers (households and businesses) worldwide. All eleven TV5 channels were dark for three hours before a temporary data feed was established to put something on customer TV screens. It took over a week to clean the network of all the hacker malware and begin work on improving security. Other French media companies were informed of the threat and joint efforts were underway to improve security. Whatever enthusiasm there was for better security will probably not last because this was not the first time something like this has happened.

It's not that the threat was ignored or underestimated. Officially the hacker threat is taken very seriously by media companies, especially those who broadcast via satellite. Starting in the late 1990s, growing reliance on data networks and satellite distribution of programming resulted in more and more attacks on these networks by groups seeking to get some attention by briefly seizing control of or shutting down these systems.

These attacks reached something of a crescendo in 2007 when a Chinese satellite television channel was taken over by hackers. For about 90 minutes, the government had no control over the feed, which was replaced by anti-government material. The Chinese government tried to keep details of how this happened out of the news but because over 130 million Chinese then had access to the Internet and even more had cell phones it was impossible to completely black out details of what happened. Senior officials were quite upset, especially because since 2002 there had been over a dozen incidents worldwide of hijacking satellite television signals. Several of these took place in China, but until 2007 the government assured everyone that the "problem" was fixed.

After 2000 the increasing number of incidents of space satellites being "hacked" was believed to be largely the result of an increase in the number of satellites up there, and the number of ground stations broadcasting information up into the sky. Many of these early "hacks" turned out to be satellite signals interfering with one another. Same with cases where people believe their GPS or satellite communications signals were being jammed. On further investigation, the real reasons tend to be less interesting and a lot more technical. All this usually had a large element of human error mixed in. But some of the disruptions were deliberate.

The 2007 China incident clearly indicated a security problem. If you have the proper passwords and security information, you can send commands to the satellite and do whatever you want. The Chinese had a security problem and to Chinese rulers that was more frightening than, well, just about anything. China has since greatly improved its satellite security but as TV5 discovered that is not always enough. Russian EW developers watched all this with great interest and considered the possibility of improving and "weaponizing" these hacking capabilities.

Read the rest here:

https://strategypage.com/htmw/htspace/articles/20190529.aspx

Artificial intelligence, cybersecurity talent top list of hard-to-find skills

By Joe McKendrick, ZDNet, May 25, 2019

Application development workloads keep growing, but developer teams are not. If anything, development skills are increasingly in precious short supply.

That's the word from the latest survey of 3,300 IT leaders, conducted by OutSystems. The development skills shortage has been a crisis raging for a number of years now, and this latest survey shows no sign of abating.

Fueling the demand is the rising tide of digital transformation, and with it, the reliance of business leaders on technology to amp up the customer experience and compete on data analytics. The number of applications respondents have slated for delivery in 2019 is 60% higher than in last year's survey. A majority, 65%, said they had plans to deliver 10 or more applications, 38% plan to deliver 25 or more apps, and 15% said they plan to deliver 100 or more apps in 2019.

While demand for applications is up, development teams are not growing to meet the demand. Only 36% of the organizations in the survey have larger application development teams than a year ago.

Still, development teams are getting better at getting applications designed, built, tested and out the door. A majority of IT managers, 61%, report that it takes four months or less to deliver an application -- up from 54% a year ago. However, backlogs remain stubbornly long. Close to two-thirds of IT professionals, 64%, say they have an app dev backlog, and for 19% of these respondents, the backlog was more than 10 apps. Only 39% said their app dev backlog had improved in the last year, and 50% say it's about the same.

Finding enough people to cut through these backlogs to build and deliver these applications has grown even more difficult. Only 15% of IT managers describe such recruitment as easy, and for many specialties, recruitment was described as hard or very hard. A majority of IT managers report that it is difficult or "very difficult" to find or train for the following skills:

- Artificial Intelligence/machine learning specialist 72%
- Cybersecurity specialist 64%
- IoT Specialist 56%
- Full-Stack Developer 56%
- BI/Analytics data scientist specialist 52%
- API/Integration/backend developer 45%

When it comes to training priorities in the year ahead, web development, mobile development, and API/integration/backend topped the list.

Read the rest here:

https://www.zdnet.com/article/artificial-intelligence-cybersecurity-talent-top-list-of-hard-to-find-skills/

Update Your Profile!

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

SPECIAL INTEREST GROUPS (SIGS)

Special Interest Groups (SIGs) are groups comprised of Cybersecurity professionals who gather together to share information and experiences common to their respective groups. ISSA-COS presents SIGs in two major categories: Affinity Groups and Industry Groups. On a quarterly basis, ISSA-COS brings together both groups to participate in formally structured events. During these gatherings, participants have an opportunity to first attend one of four (4) Affinity Groups then, one of four (4) Industry Groups. CPEs/CPUs are awarded for attend these events.

In-between formal gatherings, the SIG Leaders for each individual SIG are encouraged to coordinate informal gatherings. ISSA-COS encourages SIG leaders to consider hosting informal gatherings at social venues such as sporting events, restaurants, bars, or breweries. Informal gatherings may also include participating in a community improvement project, a group walk or hike, or a picnic/BBQ.

Affinity Groups

Affinity Groups are designed for community professionals with like-minded interests in the field of Cybersecurity. Affinity Groups gather to share security related experiences, impart knowledge and education, and help one another solve common problems and issues. The Affinity Groups currently promoted by ISSA-COS include:

Women in Security – **W***[omen]***IS**

Young Professional in Security – **Y***[oung Professionals]***IS**

Mentoring in Security – **M***[entoring]***IS**

Executives in Security – **E***[xecutives]***IS**

Industry Groups

Industry Groups are designed for community professionals who work within similar industries and have a common interest in Cybersecurity. Industry Groups gather together to discuss security related topics and share solutions to problems affecting their perspective industries. They also exchange Cybersecurity related tips, information, and education specific to their industries. The Industry Groups currently promoted by ISSA-COS include:

Finance in Security – **F***[inance]***IS**

Healthcare in Security – **H***[ealthcare]***IS**

Retail in Security – **R***[etail]***IS**

DoD in Security – **D***[oD]***IS**

ISSA-COS invites you to join us at our next SIG gathering or any one of our many other events.

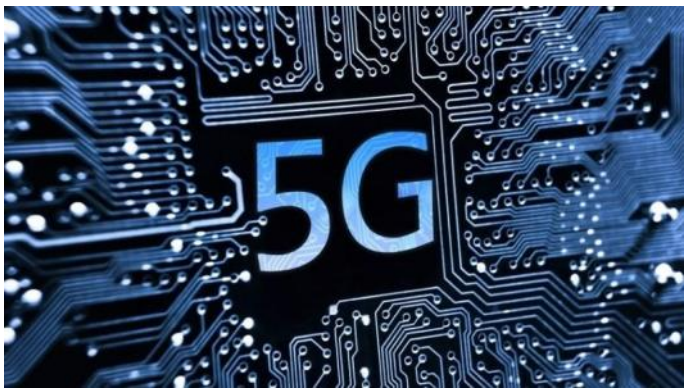
For additional information, contact: info@issa-cos.org or visit www.issa-cos.org.

The Overlooked Military Implications of the 5G Debate

By Erica Borghard, Real Clear Defense, May 6, 2019

Last week, the U.S. Defense Innovation Board released a report outlining the risks and opportunities for the United States in the global race to develop 5G. This followed a damning report published by the United Kingdom's Huawei Cyber Security Centre Oversight Board detailing how the Chinese telecom giant's 5G products, particularly its software, contained significant vulnerabilities and that the company had failed to remedy persistent poor security practices. 5G network architecture uses high frequency spectrum to enable significantly faster speeds to process larger amounts of data with lower latency and greater device connectivity. While much attention has been paid to economic and espionage implications of a potential Chinese lead in developing and operating 5G infrastructure, there are important military implications that remain largely overlooked.

There are economic implications for which entities can secure the greatest global market share of 5G technology. Technological innovation drives economic growth, job creation, and global economic influence. Huawei may have a long-term market advantage over U.S and Western telecoms because the former has been able to offer 5G products at far cheaper rates than the latter. Furthermore, there are also concerns that Chinese-built 5G technology is likely to contain backdoors that could be used to enable Chinese economic or national security espionage. It is unlikely that Beijing would actively monitor all of the content of the data that comes across Huawei owned or operated infrastructure (although it may collect and analyze metadata). However, it is conceivable that Huawei would get a proverbial "tap on the shoulder" from Beijing to share pertinent information in specific instances. This may include individually targeting senior corporate executives, which is enabled by the millimeter wave frequency that 5G networks employ.



The military applications of 5G technology have vital strategic and battlefield implications for the U.S. Historically, the U.S. military has reaped enormous advantages from employing cutting edge technology on the battlefield. 5G technology holds similar innovative potential. Perhaps most obviously, the next generation of telecommunications infrastructure will have a direct impact on improving military communications. However, it will also produce cascading effects on the development of other kinds of military technologies, such as robotics and artificial intelligence. For instance, artificial intelligence and machine learning capabilities, such as those used in the Department of Defense's Project Maven, could be greatly enhanced when leveraging the data processing speeds made possible through 5G infrastructure. As an era of great power competition emerges between the United States and China, the United States has a compelling strategic interest in being at the forefront of these new technologies.

The United States and its allies must also consider the tactical and operational implications on the battlefield of conducting conventional or counterinsurgency operations in an area with Chinese owned or operated 5G infrastructure. This concern stems from the nature of the relationship between Huawei, an ostensibly private company, and the Chinese Communist Party (CCP). While Huawei's founder and CEO, Ren Zhengfei proclaimed in a February 2019 interview on CBS This Morning that the company never has and never would provide information to the Chinese government, many experts are skeptical. Under China's 2017 National Intelligence Law, the CCP has the authority to monitor and investigate domestic and international companies as well as direct organizations to assist with government espionage efforts. As such, it is conceivable that Huawei will be required to hand over its data to the Chinese government for collection and analysis.

Due to this reality, the United States must consider and be prepared to conduct overseas contingency or counterterrorism operations in areas where Chinese telecommunications infrastructure is widely proliferated, thus restricting the United States' ability to rely on indigenous telecoms. As noted by US AFRICOM Commander General Thomas Waldhauser, this has already become an issue in Africa where Chinese telecommunications companies are poised to dominate. The integrity of U.S. military communications systems that rely on 5G networks could be undermined at key phases of an operation. For example, if the United States is conducting a military operation in an area of interest to China, it is plausible that the Chinese government could leverage Huawei to intercept or even deny military communications. Furthermore, Chinese telecom infrastructure dominance in a theater of operations may limit the U.S. military's ability to conduct precision targeting that leverages signals intelligence collection on 5G telecommunications networks.

Read the rest here:

https://www.realcleardefense.com/articles/2019/05/06/the_overlooked_military_implications_of_the_5g_debate_114395.html

'Deep fake' videos that can make anyone say anything worry U.S. intelligence agencies

By Joe Toohey, Fox 5 NY, May 8, 2018

A video of a seemingly real news anchor, reading a patently false script saying things like the "subways always run on time" and "New York City pizza is definitely not as good as Chicago" gives a whole new meaning to the term fake news.

But that fake news anchor is a real example of a fascinating new technology with frightening potential uses.

I was stunned watching the Frankenstein mix of Steve Lacy's voice coming out of what looks like my mouth.

The video is what is known as a deep fake: a computer-generated clip using an algorithm that learned my face so well that is can recreate it with remarkable accuracy.

My generated face can be swapped onto someone else's head (like that original video with Steve) or it can be used to make me look like I'm saying things I've never said.

For this piece, I worked with Lyu and his team at the College of Engineering and Applied Sciences at the University at Albany.

For many people, seeing is believing.

"I would say it's not 100% true anymore," Lyu said.

Their deep fake research is funded by the Defense Advanced Research Projects Agency, or DARPA, which acts as the research and development wing of the U.S. Defense Department. They're working to develop a set of tools the government and public can use to detect and combat the rise of deep fakes.

"What we're doing here is providing a kind of detection method to authenticate these videos," Lyu said.

What's more, deep fakes technically aren't that hard to make. All it takes is a few seconds of video of someone, a powerful computer, and some code, which Lyu and his team don't release publicly.

"The real danger, I believe, is the fact that the line between what is real and what is fake is blurred because of the existence of this kind of technology," Lyu said.

But it is about more than just a news anchor face-swap experiment. The power to make a video of anybody saying anything is alarming.

Even the former president is raising red flags. The funny thing is (as you see in the video) that is not Barack Obama. The video is a deep fake. Actor Jordan Peele is impersonating Obama's voice. The algorithm is doing the rest. It's meant to be a PSA about the dangers of deep fakes.

"Moving forward we need to be more vigilant with what we trust from the internet," fake Obama warns.

Imagining how a deep fake video could quickly create a very scary real-world scenario is not hard.

Say, for instance, a video of a world leader, such as Vladimir Putin, pops up on the internet declaring war on another country, or, maybe, the head of a major company announcing his or her abrupt resignation, putting the markets in a tail spin.

Videos like that can spread like wildfire before fact checkers, journalists, and governments even have the chance to authenticate it.

And the U.S. government is paying attention. Deep fakes were a topic at the recent worldwide threats hearing in front of the Senate Intelligence Committee.

"Are we organized in a way where we could possibly respond fast enough to a catastrophic deep fakes attack?" Sen. Ben Sasse, a Nebraska Republican, asked a panel of the heads of the nation's intelligence agencies.

Director of National Intelligence Dan Coats responded by saying emerging technology like deep fakes pose "a major threat to the United States and it's something the intelligence community needs to be restructured to address."

House Intelligence Committee member Sean Patrick Maloney told Fox 5 News, "You ain't seen nothing yet."

Read the rest here:

http://www.fox5ny.com/news/deep-fake-videos-intelligence-agencies

Newly Released Amazon Patent Shows Just How Much Creepier Alexa Can Get

By Peter Dockrill, Science Alert, May 28, 2018

A newly revealed patent application filed by Amazon is raising privacy concerns over an envisaged upgrade to the company's smart speaker systems. This change would mean that, by default, the devices end up listening to and recording everything you say in their presence.

Alexa, Amazon's virtual assistant system that runs on the company's Echo series of smart speakers, works by listening out for a 'wakeword' that tells the device to turn on its extended speech recognition systems in order to respond to spoken commands.

On Amazon's devices, the wakeword is 'Alexa', but similar systems control how Apple devices work ('Hey Siri') and also Google's ('Hey Google'), not to mention products from other tech companies.

In theory, Alexa-enabled devices will only record what you say directly after the wakeword, which is then uploaded to Amazon, where remote servers use speech recognition to deduce your meaning, then relay commands back to your local speaker.

But one issue in this flow of events, as Amazon's recently revealed patent application argues, is it means that anything you say before the wakeword isn't actually heard.

"A user may not always structure a spoken command in the form of a wakeword followed by a command (eg. 'Alexa, play some music')," the Amazon authors explain in their patent application, which was filed back in January, but only became public last week.

"Instead, a user may include the command before the wakeword (eg. 'Play some music, Alexa') or even insert the wakeword in the middle of a command (eg. 'Play some music, Alexa, the Beatles please'). While such phrasings may be natural for a user, current speech processing systems are not configured to handle commands that are not preceded by a wakeword."

To overcome this barrier, Amazon is proposing an effective workaround: simply record everything the user says all the time, and figure it out later.

Rather than only record what is said after the wakeword is spoken, the system described in the patent application would effectively continuously record all speech, then look for instances of commands issued by a person.

"The [proposed] system is configured to capture speech that precedes and/or follows a wakeword," the application explains, "such that the speech associated with the command and wakeword can be included together and considered part of a single utterance that may be processed by a system."

It's actually a clever idea, similar as others have noted to Apple's introduction of its Live Photos feature in the iPhone in 2015.

In that implementation, as soon as you open the iPhone's Camera app, the camera starts surreptitiously filming footage, even before you hit the shutter button icon to take your photo.

In fact, even once you've hit the shutter button, the camera keeps recording, and you ultimately end up with a mini movie (aka 'Live Photo') that extends for a moment on either side of the still image you manually snapped.

The proposed Alexa upgrade – which isn't necessarily something Amazon will ever roll out in its products – brings the same kind of thinking to recorded audio, ostensibly just so it never misunderstands you when you say something like, "Play some music, Alexa, the Beatles please".

It's worth noting, too, that the envisaged feature wouldn't send everything it records to Amazon's servers.

In the patent application, the authors explain that your Echo device would only ever record between 10–30 seconds of audio at a time, before wiping it from the local memory buffer, and recording a new 10–30 seconds of audio over it (again and again).

Read the rest here:

https://www.sciencealert.com/creepy-new-amazon-patent-would-mean-alexa-records-everything-you-say-from-now-on

Inside the Government's Open Source Software Conundrum

By ack Corrigan, Nextgov, May 22, 2019

On July 29, 2017, the IT security team at Equifax noticed some unusual activity on one of the credit bureau's public websites. The team blocked the suspicious traffic, but the next day, it came back.

The company started formally investigating the situation a few days later, but at that point it was too late. Hackers had already made off with sensitive data on millions of people, including the names, birthdays and Social Security numbers of nearly half the U.S. population.

The Equifax incident, which stands as the fifth largest data breach in history, grew out of a bug in the open source code the company used to build an application for people to dispute credit reports. The Homeland Security Department notified Equifax about the vulnerability in the Apache Struts software in March 2017, but the company never fixed the bug, leaving wide open a door that hackers used for more than two months to scoop up records on 145 million people.

The breach highlights one of the most pressing issues facing the cybersecurity community today: How do government agencies and private companies make sure the open source software that underlies nearly every piece of tech on the market is safe to use?

Inside the Open Source Supply Chain

For people unfamiliar with the software development world, open source software is essentially chunks of code that are available online for anyone to use. While many non-coders may think software is written from scratch, in fact, much of the modern development process involves piecing together these blocks of code to create new applications. It's kind of like building with Legos: You can stack the blocks in infinite ways, but you don't mold the plastic yourself.

The popularity of open source software has exploded in recent years to keep up with the growing demand for fresh tech, according to Derek Weeks, vice president of the software security company Sonatype. The system allows developers to churn out more code in less time and prevents them from constantly recreating the wheel, he said.

"Every bit of software in every single market and every single agency is using open source components. It's so ubiquitous now," Weeks told *Nextgov*. Researchers at Sonatype estimate80 to 90 percent of every modern application is comprised of open source components.

But despite its efficiency, open source development could also pose serious cybersecurity issues. If a block of open source code contains a vulnerability, developers who use it are unknowingly building the bug into their software. And that happens pretty often.

For the popular open source coding language Java, Sonatype found about 10 percent of individual software components contain a known vulnerability, and other coding languages are no safer. In a recent survey, some 25 percent of developers in government and industry said their organization suffered a security breach as a result of an open source vulnerability in the past year, up more than 70 percent from 2014.

Historically, the tech community assumed open source code was comparatively secure because it's touched by so many different developers, but that's not necessarily the case, according to Emile Monette, a cyber supply chain risk specialist at the Cybersecurity and Infrastructure Security Agency. Most open source developers focus more on functionality than security, and don't always keep up with the latest vulnerabilities and updates, he told *Nextgov*.

As such, it can be difficult for agencies to know if the software they're buying contains an open source vulnerability that's been overlooked by the vendor. And beyond known bugs, it's likely there are even more components carrying defects that have yet to be discovered.

"No one can write perfect code," Weeks said. "All code everywhere, anywhere, whether it's an open source component or written from scratch, probably has a security flaw in it somewhere."

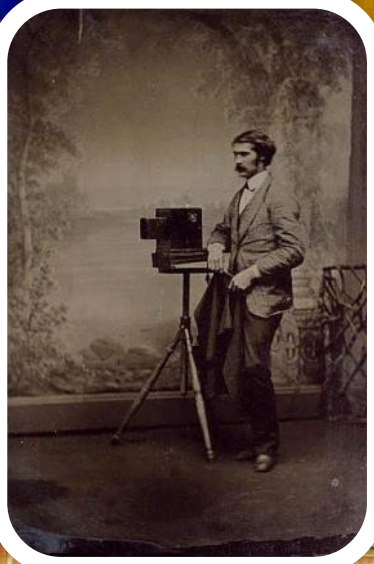
How to Squish a Bug

Read the rest here:

https://www.nextgov.com/cybersecurity/2019/05/inside-governments-open-source-software-conundrum/157186/

ISSA Photos are courtesy of our Chapter Photographer

Warren Pearce



Huawei, the US ban, and links to Chinese spying explained

By Rich Haridy, New Atlas, May 22, 2019

On May 15, 2019, US President Donald Trump declared a national emergency, signing an executive order banning US companies and government agencies from utilizing telecommunications equipment that pose a risk to national security. While the initial announcement did not mention Huawei by name, members of congress didn't hesitate to reference the massive Chinese company directly.

Soon after Trump's announcement the US Commerce Department added Huawei to what is referred to as the Entity List. Covering everything from businesses to individuals, placement on the list essentially bans an entity from doing business in the United States. There is little doubt the initial executive order was primarily geared at restricting Huawei's ability to do business in the United States.

Within days of the government action, the repercussions for Huawei began to hit hard. Google quickly ended its business dealings with the Chinese company, meaning Huawei would have no early access to the Android ecosystem, ultimately locking its smartphones out of the Google Play Store and apps like Gmail and Maps. Intel, Broadcom and Qualcomm all reportedly ceased business with Huawei, cutting off the supply of hardware fundamental to several of the company's major products.

These dramatic events were the culmination of years of suspicion surrounding Huawei's ties to the Chinese government. For well over a decade the company has been accused by governments around the world of working with Chinese national spy agencies. But what evidence is there to back up these serious claims, and what are the repercussions of this new US Huawei ban?

Long standing ties

Huawei's deep ties with the Chinese government go all the way back to the company's founding in 1987. Ren Zhengfei, Huawei's founder, has long been deeply connected with the Chinese government, working as an engineer for the People's Liberation Army before moving into commercial electronics in 1983. Through the 1990s Huawei demonstrated strong ties with the Chinese government, and by 1996 it was labeled a "national champion" following major contracts to construct the country's national telecommunications network. Alongside this, experts have claimed the growth of the company has been financially supported by Chinese state agencies – an allegation the company has consistently denied.

For years Huawei has been beset by international legal issues. From accusations of intellectual property theft, to major international sanction violations, the company inarguably has a messy record of operating on the fringes of global law. Perhaps the most dramatic development was the arrest of Huawei's Chief Financial Officer in late 2018. Meng Wanzhou, daughter of Huawei founder Ren Zhengfei, was arrested in Canada on charges of bank fraud at the request of the US.

Wanzhou is currently entrenched in a Canadian court battle as the United States attempts to extradite her, while her lawyers, and the Chinese government, claim the entire exercise is simply an attempt by Western governments to stifle the success of Huawei's international business dealings.

Unrelated to Wanzhou's legal troubles, and the company's other criminal and civil problems, many countries around the globe are slowly introducing bans on Huawei technology based on a single allegation ... that the company's independence and integrity has been compromised by the Chinese government and its technology is being used to spy on other countries.

Is there any actual evidence of spying?

Over the last decade these spying allegations have consistently hounded Huawei, however, no clear evidence has ever been presented to prove there are backdoors or surveillance spyware installed on any Huawei devices. An expansive 18-month security review from US government agencies was reported to have concluded in 2012 that there was no evidence Huawei was working with the Chinese government to spy on US citizens.

Experts working on the US government review at the time suggested that, while no singular "smoking gun" could be found proving Huawei equipment had been compromised, its systems were "riddled with holes." These coding errors and vulnerabilities were found to make some of Huawei's equipment more open to being hacked, however, no one could establish whether these were simple software mistakes or explicit backdoors left open for espionage reasons.

Read the rest here:

https://newatlas.com/huawei-ban-us-what-spy-evidence-exists/59772/?utm_medium=email&utm_campaign=2019-05-22%20143139%20USA%20Daily%20Basic%202019-05-22%20143539%20Placental%20stem%20cells%20found%20to%20regenerate%20heart%20cells%20after%20heart%20attack&utm_content=2019-05-22%20143139%20USA%20Daily%20Basic%202019-05-22%20143539%20Placental%20stem%20cells%20found%20to%20regenerate%20heart%20cells%20after%20heart%20attack+CID_ec118ac47af2cd3c78e24985680ff771&utm_source=Campaign%20Monitor&utm_term=Read%20more

Information Systems Security Association
Developing and Connecting Cybersecurity Leaders Globally
Colorado Springs Chapter

WWW.ISSA-COS.ORG

The Information Systems Security Association (ISSA) ® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

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

Article for the Newsletter?

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

Send your article ideas to the Newsletter at:

newsletter@issa-cos.org

Chapter Officers:

President*: Ernest Campos
Vice President*: Michael Crandall
Executive Vice President*: Scott Frisch
Treasurer: Mark Maluschka
- Deputy Treasurer: Vacant

Recorder/Historian: Mike Daetwyler
- 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: David Reed
- Deputy: Melissa Absher

Vice President of Training: Mark Heinrich
- Deputy: Jeff Tomkiewicz

Member at Large: James Asimah
Member at Large: Bill Blake
Member at Large: Jim Blake
Member at Large: **Vacant**

Committee Chairs:

Training: Mark Heinrich
Hospitality: Stephen Parish
Mentorship Committee Chair: Carissa Nichols
Ethics: Timothy Westland
Recognition: **Vacant**
Media: Don Creamer
IT Committee: Patrick Sheehan
Speaker's Bureau: William (Jay) Carson

Executive Assistant: Andrea Heinz

** Executive Board Members*

Significant Interest Group Leads:

Chair: **Vacant**
Women in Security : June Shore
Young Prof. in Security: Jeremiah Walker
Educators in Security: **Vacant**
Executives in Security: **Vacant**
Finance in Security: **Vacant**
Healthcare in Security: Dennis Schorn
Retail in Security: **Vacant**
DoD in Security: Steven Mulig

Past Senior Leadership

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

US Air Force probes targeted malware attack, blames... er, the US Navy? What?

By Gareth Corfield, The Register, May 22, 2019

The US Air Force has opened an investigation into a "malware" infection – which it is blaming on lawyers employed by the US Navy who are working on a war crimes case.

The bizarre case hinges around an alleged attempt by a US Navy prosecutor to plant malware on the devices of US Air Force lawyers defending a US Navy SEAL over war crimes charges from his time commanding a small unit in Afghanistan.

Read the rest here:

https://www.theregister.co.uk/2019/05/22/us_navy_us_air_force_friendly_fire_malware_allegations/

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