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

ISSA-COS NEWSLETTER

VOLUME 9 NUMBER 3 MARCH 2020

Colorado Springs, Colorado

Good Things Coming!

A Note From Our President

By Mr. Ernest Campos

Fellow Members of ISSA-COS,

As you "*Beware of the Ides of March,*" don't miss out on all the good things such as… St. Patrick's Day, Corned Beef and Cabbage, Green Beer, National Pi Day, and College Basketball… lots of college basketball! For ISSA-COS, March is a special month for other reasons. March is the month we celebrate our first conference of the year. It is also the month we break from normal monthly programming and host or participate in special events. Finally, it is the month we regroup and recharge before the 2nd quarter starts.

Looking back at February, we enjoyed dinner and lunch presentations from **Mr. William "Bill" Vivian**, a Cybersecurity Leadership Coach and Founder of Freestone Solutions Group, LLC. Bill's presentation was entitled "**How Engaged Employees Secure a Network**" and it was very well received by those who attended. There were lots of questions, discussions, and sharing of professional experiences among the attendees. At our Mini Seminar, **Mr. Justin Whitehead**, CEO of Digital Silence, provide us with a double feature presentation entitled "**Network Scanning and Exploits**." Here too, attendees shared lots of tips and techniques while learning and practicing on various tools. The Saturday Mini Seminar also marked our second event held at Pikes Peak Community College – Rampart Range. If you attended the January Mini Seminar, you likely witnessed us experiencing many challenges. Fortunately, we worked out a lot of kinks and February was a much better experience. Apart from our scheduled presentations, our Board of Directors (BoD) remained active reviewing new opportunities for members of our chapter and our community to engage in meaningful events in the months to come. We are excited about all that is in store for the rest of the year and hope many of you will find time to participate.

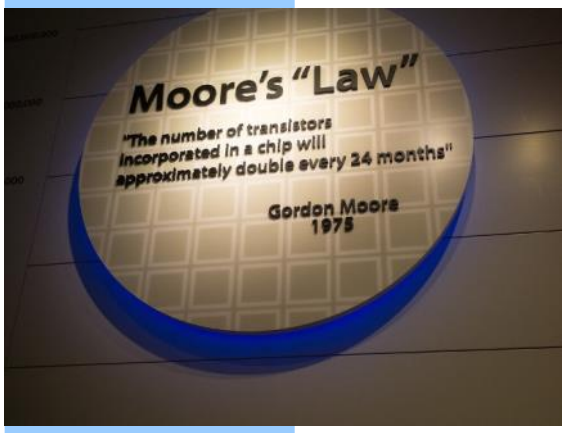
Back to this month though, in March we will participate in Women in Cybersecurity (WiCyS) conference being held at the Denver Gaylord Convention Center from the 12th – 15th. On the 13th and 14th, ISSA-COS will be assisting with the WiCyS Career Village by providing resume reviews, career coaching, mock interviews, and other types of soft skills advice. Later in March, ISSA-COS will host the 7th Annual Cyber Focus Days Symposium at UCCS. This event will take place

(Continued on page 4)

We're not prepared for the end of Moore's Law

By David Rotman, MIT Technology Review, February 24, 2020

Gordon Moore's 1965 forecast that the number of components on an integrated circuit would double every year until it reached an astonishing 65,000 by 1975 is the greatest technological prediction of the last half-century. When it proved correct in 1975, he revised what has become known as Moore's Law to a doubling of transistors on a chip every two years.



Since then, his prediction has defined the trajectory of technology and, in many ways, of progress itself.

Moore's argument was an economic one. Integrated circuits, with multiple transistors and other electronic devices interconnected with aluminum metal lines on a tiny square of silicon wafer, had been invented a few years earlier by Robert Noyce at Fairchild Semiconductor. Moore, the company's R&D director, realized, as he wrote in 1965, that with these new integrated circuits, "the cost per component is nearly inversely proportional to the number of components." It was a beautiful bargain—in theory, the more transistors you added, the cheaper each one got. Moore also saw that there was plenty of room for engineering advances to increase the number of transistors you could affordably and reliably put on a chip.

"It's over. This year that became really clear."

Soon these cheaper, more powerful chips would become what economists like to call a general purpose technology—one so fundamental that it spawns all sorts of other innovations and advances in multiple industries. A few years ago, leading economists credited the information technology made possible by integrated circuits with a third of US productivity growth since 1974. Almost every technology we care about, from smartphones to cheap laptops to GPS, is a direct reflection of Moore's prediction. It has also fueled today's breakthroughs in artificial intelligence and genetic medicine, by giving machine-learning techniques the ability to chew through massive amounts of data to find answers.

But how did a simple prediction, based on extrapolating from a graph of the number of transistors by year—a graph that at the time had only a few data points—come to define a half-century of progress? In part, at least, because the semiconductor industry decided it would.

Moore wrote that "cramming more components onto integrated circuits," the title of his 1965 article, would "lead to such wonders as home computers—or at least terminals connected to a central computer—automatic controls for automobiles, and personal portable communications equipment." In other words, stick to his road map of squeezing ever more transistors onto chips and it would lead you to the promised land. And for the following decades, a booming industry, the government, and armies of academic and industrial researchers poured money and time into upholding Moore's Law, creating a self-fulfilling prophecy that kept progress on track with uncanny accuracy. Though the pace of progress has slipped in recent years, the most advanced chips today have nearly 50 billion transistors.

Every year since 2001, MIT Technology Review has chosen the 10 most important breakthrough technologies of the year. It's a list of technologies that, almost without exception, are possible only because of the computation advances described by Moore's Law.

For some of the items on this year's list the connection is obvious: consumer devices, including watches and phones, infused with AI; climate-change attribution made possible by improved computer modeling and data gathered from worldwide atmospheric monitoring systems; and cheap, pint-size satellites. Others on the list, including quantum supremacy, molecules discovered using AI, and even anti-aging treatments and hyper-personalized drugs, are due largely to the computational power available to researchers.

But what happens when Moore's Law inevitably ends? Or what if, as some suspect, it has already died, and we are already running on the fumes of the greatest technology engine of our time?

Read the rest here:

https://www.technologyreview.com/s/615226/were-not-prepared-for-the-end-of-moores-law/

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.

New Members February
Rodney Gullatte Jr.
John Geiger
Dan Lee
Christopher Scheirer
James Madden
Alexander Johnson
Lindsey Chernoff
Joseph Rogers
Kyle Damon
Patricia March
Sean Callahan

Welcome to 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.

Our membership is hanging it at ~400 members as of the end of February.

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

Vice President of Membership

membership@issa-cos.org

Membership Fun Facts

Top three ZIP codes for membership in our chapter:

1. 80831 – Peyton Area
2. 80920 – Briargate Area
3. 80918, 80922, 80923 – The Power Zone
   - Cimarron Hills
   - Springs Ranch
   - Stetson Hills

Keep making those membership referrals! **Invite a guest for free.**

Please update your Bio and Email (one that you always monitor) on the ISSA International website

(Continued from page 1)

A Note From Our President

from the 25th – 26th and will feature a Capture-the-Flag (CTF)/Boss of the SOC challenge sponsored and facilitated by **Splunk and Epoch Concepts** on Day 1 and a stellar line up of guest speakers including a two-hour Artificial Intelligent workshop hosted by **HP Enterprise** on Day 2. As of the time of this letter, additional sponsors for this event include **Murray Security Services (Platinum), Jacobs (Bronze), and UCCS (Venue).** More information about this event can be found in this newsletter. Please don't delay and take advantage of the early bird registration period. **Registration is free for all members of ISSA and those in the .gov, .mil, and .edu communities.** Sponsorship opportunities are still available so please help spread the word.

As we look even further down the road, 2021 will mark the 30th Anniversary of our chapter's existence! In preparation for this milestone year, our chapter Recorder/Historian, Andrea Heinz, is spending all of 2020 gathering and organizing a complete and definitive history of our chapter. Throughout the year, she will also take time to interview current and past Presidents, Board Members, General Members, and External Organizations. If you would like to contribute to this project, please reach out to Andrea at Recorder@issa-cos.org. She will gladly schedule a phone interview with you to collect your stories and contributions. Behind the scenes, our Board of Directors is already planning for one fantastic celebration.

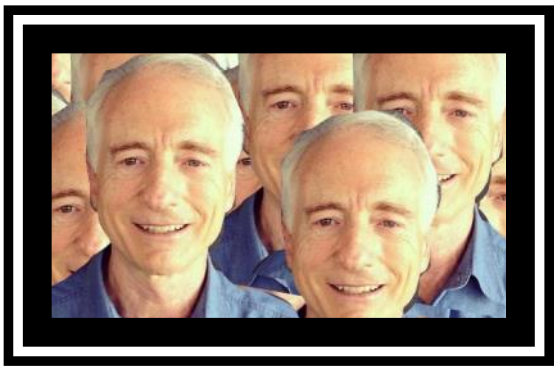
Last of all, I want to take a moment to acknowledge a significant event taking place in Pueblo, CO. In the month of February, a team of Cybersecurity leaders and professionals fulfilled the final requirements necessary to apply for chapter-hood with ISSA International. Pending approval, Pueblo will become the fourth ISSA chapter in our great state of Colorado. For nearly 6-months, our chapter has been serving as "Big Brother" to Pueblo while they initiated this effort and as such, we are very proud of them. ISSA-COS will continue to mentor Pueblo as they continue to establish their presence within their community and within our state.

In closing, I extend a heartfelt "**thank you**" to all our general members for your constant support and feedback. Your attendance at scheduled events is very important for the continued strength of our chapter. We also appreciate your volunteerism and generosity of time and funds. Without your support, our chapter would not be thriving as it is today. Please continue to send us your comments and feedback; both good and bad. Then, give us time and opportunity to solidify the things we are doing right and improve upon the things we need to fix. On behalf of the Board, we wish you all a great month of March!

Sincerely,

Ernest

Pioneer who invented 'cut, copy and paste' for computers dies at 74



By Sommer Brokaw, UPI, February 20, 2020

Larry Tesler, a former chief scientist for Apple and the man who invented the concepts for computers to cut, copy and paste, died this week. He was 74.

Born in New York City in 1945, Tesler eventually studied computer science at Stanford University before working in the school's artificial intelligence research lab in the late 1960s. He moved to Xerox in 1973, where he devised the time-saving concepts to cut, copy and paste in computer systems.

"Your workday is easier thanks to his revolutionary ideas," Xerox tweeted Thursday to honor Tesler.

Tesler left Xerox and joined a then-young Apple Computer in 1980 -- making the move, he said later, because Apple founder Steve Jobs was clearly innovating toward personal computers, whereas Xerox had still considered itself a copier company. He became Apple's chief scientist and remained there until 1997.

Tesler also promoted "modeless" computing, a concept under which computers operate in a single mode rather than switch between various user-defined modes. His advancements for cut, copy and paste were later heavily utilized by Apple's Macintosh personal computer in the early 1980s.

Read the rest here:

https://www.upi.com/Top_News/US/2020/02/20/Pioneer-who-invented-cut-copy-and-paste-for-computers-dies-at-74/2041582220436/

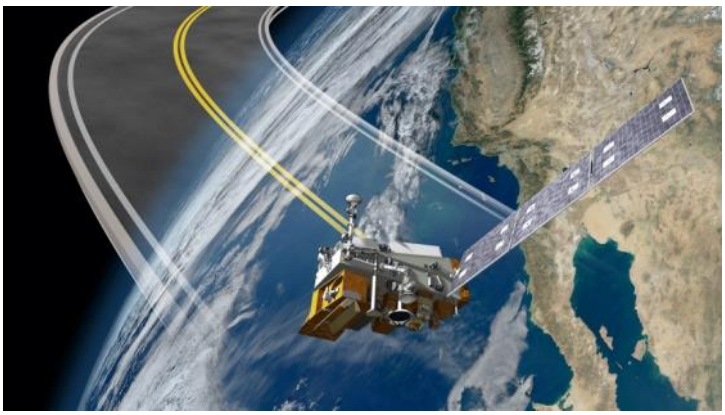
Hackers could shut down satellites – *or turn them into weapons*

By Prodita Sabarini , The Conversation, February 12, 2020

Last month, SpaceX became the operator of the world's largest active satellite constellation. As of the end of January, the company had 242 satellites orbiting the planet with plans to launch 42,000 over the next decade. This is part of its ambitious project to provide internet access across the globe. The race to put satellites in space is on, with Amazon, U.K.-based OneWeb and other companies chomping at the bit to place thousands of satellites in orbit in the coming months.

These new satellites have the potential to revolutionize many aspects of everyday life – from bringing internet access to remote corners of the globe to monitoring the environment and improving global navigation systems. Amid all the fanfare, a critical danger has flown under the radar: the lack of cybersecurity standards and regulations for commercial satellites, in the U.S. and internationally. As a scholar who studies cyber conflict, I'm keenly aware that this, coupled with satellites' complex supply chains and layers of stakeholders, leaves them highly vulnerable to cyberattacks.

If hackers were to take control of these satellites, the consequences could be dire. On the mundane end of scale, hackers could simply shut satellites down, denying access to their services. Hackers could also jam or spoof the signals from satellites, creating havoc for critical infrastructure. This includes electric grids, water networks and transportation systems.



Some of these new satellites have thrusters that allow them to speed up, slow down and change direction in space. If hackers took control of these steerable satellites, the consequences could be catastrophic. Hackers could alter the satellites' orbits and crash them into other satellites or even the International Space Station.

Commodity parts open a door

Makers of these satellites, particularly small CubeSats, use off-the-shelf technology to keep costs low. The wide availability of these components means hackers can analyze them for vulnerabilities. In addition, many of the components draw on open-source technology. The danger here is that hackers could insert back doors and other vulnerabilities into satellites' software.

The highly technical nature of these satellites also means multiple manufacturers are involved in building the various components. The process of getting these satellites into space is also complicated, involving multiple companies. Even once they are in space, the organizations that own the satellites often outsource their day-to-day management to other companies. With each additional vendor, the vulnerabilities increase as hackers have multiple opportunities to infiltrate the system.

Hacking some of these CubeSats may be as simple as waiting for one of them to pass overhead and then sending malicious commands using specialized ground antennas. Hacking more sophisticated satellites might not be that hard either.

Satellites are typically controlled from ground stations. These stations run computers with software vulnerabilities that can be exploited by hackers. If hackers were to infiltrate these computers, they could send malicious commands to the satellites.

A history of hacks

This scenario played out in 1998 when hackers took control of the U.S.-German ROSAT X-Ray satellite. They did it by hacking into computers at the Goddard Space Flight Center in Maryland. The hackers then instructed the satellite to aim its solar panels directly at the sun. This effectively fried its batteries and rendered the satellite useless. The defunct satellite eventually crashed back to Earth in 2011. Hackers could also hold satellites for ransom, as happened in 1999 when hackers took control of the U.K.'s SkyNet satellites.

Over the years, the threat of cyberattacks on satellites has gotten more dire. In 2008, hackers, possibly from China, reportedly took full control of two NASA satellites, one for about two minutes and the other for about nine minutes. In 2018, another group of Chinese state-backed hackers reportedly launched a sophisticated hacking campaign aimed at satellite operators and defense contractors. Iranian hacking groups have also attempted similar attacks.

Read the rest here:

http://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932

ISSA
Colorado Springs Chapter

7th ANNUAL CYBER FOCUS DAY

"Cybersecurity: Stories of Innovation and Inspiration"

www.issa-cos.org

Join the Information Systems Security Association (ISSA) - Colorado Springs Chapter for the 7th Annual Cyber Focus Day (CFD) www.issa-cos.org set to take on Wednesday, March 25, 2020 and Thursday, March 26, 2020 at the University of Colorado, Colorado Springs (UCCS) – University Center – 2nd Floor Berger Hall.

March 25th

ISSA-COS Capture the Flag (CTF)
a.k.a. "ISSA-COS CFD CTF"
9am - 1130am - CTF Prep Session
1130am -1230pm - Lunch (provided)
1230pm to 430pm - CTF Challenge

*** Prizes will be awarded for top competitor rankings*
*** Plus, best hat, best shirt, and best charm!*

March 26th

ISSA-COS Cyber Focus Day Symposium
8am - 430pm
Lunch (provided)
Keynote Speakers
Breakout Sessions
HPE AI Workshop
Exhibitor Hall (all day)

March 25 - March 26, 2020
University of Colorado - Colorado Springs (UCCS)
University Center - 2nd Floor Berger Hall

...to join us visit www.issa-cos.org

Keynote Speakers

Dr. Jim Crowder
Systems Fellow
Mad Scientist
Colorado Engineering, Inc.

Nathan Toups
Senior Site Reliability Engineer
Santé Capital
Quantitative Hedge Fund

Confirmed Speakers

"Cybersecurity Today – Latest Insights and Innovations from Your Supply Chain to Your Tactical Edge"
Sam Ceccola - Public Sector CTO Lead and Account CTO for DOD, Hewlett Packard Enterprise (HPE)

"War Stories: Penetration Testing in the DoD and Private Sector"
Todd Cronin - Lead, Commercial Cybersecurity, PLEX Solutions, LLC

"Small Business Cyber: Preventative Methods to Help Mitigate Cyber Attacks"
Rodney Gullatte Jr. - CEO, Firma IT Solutions & Services

"Cyber Insurance and Risk Assessment"
Darla Lindt - Executive Director, National Cyber Exchange (NCX)

"What You Need to Know About CMMC"
Greg Roman - CEO, SudoLynx, Inc.

"Agile Cyber"
Jordan "Cancer" Scott - Owner, Code Talkers Engineering

"Diverse Operational Security at UCCS"
Greg Williams - Director of Operations, Office of Information Technology, UCCS

"Incident Response"
Steve Winterfield - Advisory CISO, Akamia Technologies

Ways to Join Us

Attendee Fee

Early Bird Registration	$0
(visit issa-cos.org for eligibility and cut-off dates)	
Regular Registration	$99.00
Late Registration	$149.00

Exhibit and/or Sponsor

Platinum Sponsor	$4,995.00
Gold Sponsor	$3,995.00
Silver Sponsor	$2,995.00
Bronze Sponsor	$1,995.00
Exhibitor (5' x 8')	$1,495.00

...to learn more visit www.issa-cos.org

ISSA Fellow Program

2020 Fellows Cycle Now Open

The Colorado Springs ISSA Chapter has over 400 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, once the 2020 award criteria is made available please contact Colleen Murphy at past-president@issa-cos.org to 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 in the near future, and details will be provided in a future newsletter. 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 2020 ISSA International Conference.

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, we will have available the 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.

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.

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.

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.

Additional details will follow as they become available.

2020 ISSA Awards Program

ISSA annually recognizes outstanding information security professionals, their companies, and chapters that are at the top of their respective games. Who would you like to see recognized? Nominations may be made by any member. Anyone interested in making a nomination should thoroughly review the 2020 Awards Policies and Procedures once they are available.

This year's awards will be presented at the ISSA International Summit. Award winners will receive transportation, lodging, and complimentary registration. Any member in good standing is eligible to propose candidates in all categories.

In 2019 the ISSA International presented awards in these categories:

Hall of Fame: pays homage to an individual's exceptional qualities of leadership in his or her own career and organization as well as an exemplary commitment to the information security profession (ISSA membership not required).

Honor Roll: recognizes an individual's sustained contributions to the information security community, enhancement of the professionalism of ISSA members, and advancement of the association.

Security Professional of the Year: honors the member who best exemplifies the most outstanding standards and achievement in information security in the preceding year.

Volunteers of the Year: recognizes members who have made a significant difference to his or her chapter, the association, or the information security community through dedicated and selfless service to ISSA.

Chapters of the Year: rewards chapters that have done an exceptional job of supporting ISSA's mission, serving their member communities, and advancing the field. Nominees will be evaluated on their activities and programs in six areas: member services, membership development, projects and special events, development of the next generation of security professionals, communications and marketing, and participation and support of ISSA International initiatives and programs.

There are four chapter categories available for nomination:

- Small: Less than 100 members
- Medium: 100-300 members
- Large: More than 300 members
- International: Non-US Chapter (new in 2018)

Organization of the Year: acknowledges an organization that has provided a sustained, proactive presence that directly contributed to the overall good and professionalism of the association and its membership, providing services, products, and/or direct support that ensures the promotion of the highest ethical standards in addressing information security and its future direction.

President's Award for Public Service: honors an individual's contribution to the information security profession in the area of public service. (ISSA membership not required).

The 2020 Award criteria will be made available soon and will be in the chapter newsletter.

Cyberattack shut down gas pipeline *for days* – DHS

By Christian Vasquez, E&E News, February 195, 2020

A recent ransomware cyberattack caused a natural gas company to shut down a pipeline for two days, according to an alert from the Department of Homeland Security.

DHS's Cybersecurity and Infrastructure Security Agency (CISA) said yesterday it responded to the incident, but the agency did not say where or when the attack occurred. The technical document marks the first time the U.S. government has publicly reported a disruptive hack of U.S. pipeline networks.

The unspecified "threat actor" behind the attack breached the facility's network in a malicious link sent in an email, according to CISA. The malware first infected the information technology network before spreading to the operational technology network in a natural gas compression station. The hackers then triggered the ransomware, which encrypted data and blocked systems from running properly.

The operators of the facility chose to shut down a "pipeline asset" for two days, "resulting in a loss of productivity and revenue," DHS said. The hackers were able to get into the OT networks due the operators not properly dividing it from the IT systems, CISA said.

During the attack, the hackers disrupted various devices needed for operators to view what was happening in the compression station, CISA said, though "at no point did the victim lose control of operations."

The facility was able to restore the last known safe computer configurations and replace equipment, the agency said.

According to CISA, the facility lacked an emergency response plan that considered cyberthreats.

CISA said that the facility's owner "cited gaps in cybersecurity knowledge and the wide range of possible scenarios" as reasons for not having a plan for hacking threats.

Clint Bodungen, CEO and founder of the cybersecurity firm ThreatGEN, said he often sees planning oversights with his midstream customers. He also said that a lack of segmentation between IT and more sensitive OT networks is not uncommon.

"This is consistent with the industry," Bodungen said. "We go out there and do tests and vulnerability assessments for so many customers, and there are so, so many of them who are in the same boat."

'Bigger and badder' threats?

Bodungen last month reported discovering "Ryuk" ransomware attacks on five oil and gas facilities. He said he wasn't sure if the latest CISA alert is about one of those incidents, which date back to November.

The alert from CISA corresponds to warnings from cybersecurity experts who cite increasing dangers from cyberattacks on old and unpatched OT systems like those used in some pipelines and power grids.

While CISA's description of the attack was vague, Bodungen warned that if it was intentional, it could mean that the hackers have the capability to cause direct and physical damage to an oil and gas facility.

"If they had the intent, if they had the OT-specific knowledge — system-specific, process-specific knowledge — then they could do bigger and badder things," Bodungen said.

Ransomware attacks are usually indiscriminate: Hackers spread malicious links to as many people as possible in massive online campaigns. But recently, ransomware threats have become more targeted and selective, experts say — especially when it comes to cyberattacks against the energy sector.

Nathan Brubaker, senior manager of the cyber-physical intelligence team at cybersecurity firm FireEye Inc., said financially motivated criminal hacker groups have "matured" from targeting IT and business processes to OT systems and physical processes. By hitting critical networks that are needed to keep the facility running, hackers end up "inflicting maximum pain to the victim."

"As a result, they are better positioned to negotiate and can often demand much higher ransoms" to give up the key to encrypted data, Brubaker said in an email.

Read the rest here:

https://www.eenews.net/stories/1062388455

Cybersecurity warning: Almost half of connected medical devices are vulnerable to hackers exploiting BlueKeep

By Danny Palmer, ZDNet, February 18, 2020

Connected medical devices are twice as likely to be vulnerable to the BlueKeep exploit than other devices on hospital networks, putting patients and staff at additional risk from cyber attacks. This is especially concerning when healthcare is already such a popular target for hacking campaigns.

BlueKeep is a vulnerability in Microsoft's Remote Desktop Protocol (RDP) service which was discovered last year, and impacts Windows 7, Windows Server 2008 R2 and Windows Server 2008.

Microsoft issued a patch for BlueKeep after it came to light in May 2019, and security authorities including the US National Security Agency (NSA) and the UK's National Cyber Security Centre (NCSC) issued urgent warnings about patching vulnerable systems.

It was feared that BlueKeep could be deployed as a worm in a similar fashion to EternalBlue – the exploit that powered WannaCry. This cyberattack affected organisations around the world, but one of the most high-profile victims was the UK's National Health Service, which saw a number of hospital networks taken offline by the incident.

However, despite warnings over a potential repeat, large numbers of standard Windows systems – and bespoke medical devices running Windows – remain vulnerable to BlueKeep attacks.

According to figures in a new report from researchers at healthcare cybersecurity company CyberMDX, 22% of all Windows devices in a typical hospital are exposed to BlueKeep because they haven't received the relevant patches. And when it comes to connected medical devices running on Windows, the figure rises to 45% – meaning almost half are vulnerable.

Connected devices on hospital networks can include radiology equipment, monitors, x-ray and ultrasound devices, anesthesia machines and more. If these devices aren't patched, it's possible that destructive cyberattacks searching for machines vulnerable to BlueKeep could put hospital networks and patients at risk.

"Unfortunately, this isn't a 'what if' thought experiment around a worst-case scenario, but a real present-day predicament that we need to take more seriously. In 2019, at least 10 hospitals were forced to turn away patients as a result of cyberattacks. And even when hospitals don't need to turn away patients, cyber insecurity can bear a serious impact on care," Ido Geffen, vice-president of product at CyberMDX, told ZDNet.

However, patching is a particular challenge for hospitals because in many cases devices must keep running to provide patient care, and can't be taken offline to apply an update. Hospital networks are also so vast that it's easy for the IT department to lose track of assets, which could lead to devices missing out on patches.

Read the rest here:

https://www.zdnet.com/article/cybersecurity-warning-almost-half-of-connected-medical-devices-are-vulnerable-to-hackers-exploiting-bluekeep/

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.

2020 Schedule of Events

Chapter Meetings – Dinner (5:30 – 7:30 PM)

Tuesday, April 21, 2020
Tuesday, May 19, 2020
Tuesday, July 21, 2020
Tuesday, August 18, 2020
Tuesday, October 20, 2020
Tuesday, November 17, 2020

Chapter Meetings – Lunch (11:00 – 1:00 PM)

Wednesday, April 22, 2020
Wednesday, May 20, 2020
Wednesday, July 22, 2020
Wednesday, August 19, 2020
Wednesday, October 21, 2020
Wednesday, November 18, 2020

Mini-Seminars – Breakfast (8:30 – 12:00 PM)

Saturday, April 25, 2020
Saturday, May 16, 2020
Saturday, July 25, 2020
Saturday, August 22, 2020
Saturday, October 24, 2020
Saturday, November 14, 2020

ISSA-COS Conferences

Cyber Focus Day (CFD) Symposium

Wednesday, March 25, 2020
Thursday, March 26, 2020

Peak Cyber (PC) Symposium

Tuesday, September 15, 2020
Wednesday, September 16, 2020
Thursday, September 17, 2020

Security + CE Reviews

Saturday, March 7, 2020
Saturday, March 14, 2020
Saturday, March 21, 2020

Saturday, September 12, 2020
Saturday, September 19, 2020
Saturday, September 26, 2020

CISSP Review

Friday, June 5, 2020
Saturday, June 6, 2020
Saturday, June 13, 2020
Friday, June 19, 2020
Saturday, June 20, 2020
Saturday, June 27, 2020

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

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

SPECIAL INTEREST GROUPS (SIGS)

SIG Overview

The ISSA-COS Special Interest Groups (SIGs) are comprised of Cybersecurity professionals who gather to share information and experiences common to their respective groups. ISSA-COS presents SIGs in two major categories: **Affinity Groups** and **Industry Groups**. Through our online forum, ISSA-COS enables our members and the community at large to participant in thoughtfully organized and well-structured categories of conversation. Forum participants can engage in any one of eight different SIGs. Within our forum, we commission Subject Matter Experts who add increased technical knowledge to all the conversational threads.

To maintain positive behaviors within the forum, ISSA-COS has assigned a SIG Program Coordinator who monitors each SIG conversation. The SIG Program Coordinator also monitors the size and degree of participation within each SIG. Once participation reaches a sizable amount, the SIG Program Coordinator will suggest and help organize in-person meet ups. This provides SIG participants an opportunity to put virtual names with physical faces to further strengthen the bonds of interaction taking place in the virtual environment.

Affinity Groups

Affinity Groups are designed for community professionals with like-minded interests in the field of Cybersecurity. Affinity Groups 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 (WIS)
- Young Professional in Security (YIS)
- Educators in Security (EduIS)
- Executives in Security (ExecIS)

Industry Groups

Industry Groups are designed for community professionals who work within similar industries and have a common interest in Cybersecurity. Industry Groups 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 (FIS)
- Healthcare in Security (HIS)
- Retail in Security (RIS)
- DoD in Security (DodIS)

FBI warns about ongoing attacks against software supply chain companies

By Catalin Cimpanu, Zero Day, February 10, 2020

The FBI has sent a security alert to the US private sector about an ongoing hacking campaign that's targeting supply chain software providers, ZDNet has learned.

The FBI says hackers are attempting to infect companies with the Kwampirs malware, a remote access trojan (RAT).

"Software supply chain companies are believed to be targeted in order to gain access to the victim's strategic partners and/or customers, including entities supporting Industrial Control Systems (ICS) for global energy generation, transmission, and distribution," the FBI said in a private industry notification sent out last week.

Besides attacks against supply chain software providers, the FBI said the same malware was also deployed in attacks against companies in the healthcare, energy, and financial sectors.

The alert did not identify the targeted software providers, nor any other victims.

Instead, the FBI shared IOCs (indicators of compromise) and YARA rules so organizations can scan internal networks for signs of the Kwampirs RAT used in the recent attacks.

KWAMPIRS MALWARE

The Kwampirs malware was first described in a report published by US cyber-security firm Symantec in April 2018.

At the time, Symantec said a group codenamed Orangeworm had used the Kwampirs malware to similarly target supply chain companies that provided software for the healthcare sector.

Symantec said Orangeworm had been in operation since 2015 and was focused on the healthcare industry primarily.

"Orangeworm's secondary targets include Manufacturing, Information Technology, Agriculture, and Logistics," Symantec said at the time. "While these industries may appear to be unrelated, we found them to have multiple links to healthcare, such as large manufacturers that produce medical imaging devices sold directly into healthcare firms, IT organizations that provide support services to medical clinics, and logistical organizations that deliver healthcare products."

A Lab52 report released a year later, in April 2019, confirmed the Symantec findings and the group's focus on the healthcare industry.

NEW ATTACKS APPEAR TO BE TARGETING THE ICS ENERGY SECTOR

However, the FBI alert sent out last week specifically warns that attacks employing Kwampirs have now evolved to targeting companies in the ICS (Industrial Control Systems) sector, and especially the energy sector.

Read the rest here:

https://www.zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies/

Update Your Profile!

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

Cybersecurity expert: All construction data 'is an asset and should be protected'

By Jenn Goodman, Construction Dive, February 26, 2020

A recent ransomware attack on Canadian contractor Bird Construction has once again highlighted the need for cybersecurity measures in the industry.

Canadian media reports late last month said that the Ontario-based government contracting company was the victim of an incident that resulted in the encryption of company files. The incident caused no major impacts and the affected files were quickly restored, a company spokesperson said.

Nevertheless, the issue raised red flags about national security interests because the contractor is a provider of construction services for major federal and provincial projects including defense facilities and police stations. In the U.S., the Department of Defense launched a Cybersecurity Maturity Model Certification program in January to help ensure contractors on government projects have the necessary cybersecurity practices in place to protect the controlled unclassified information to which they are privy.

In addition, experts say, other data such as employee social security numbers, building plans and construction time frames is easily exploitable and can have serious legal and/or financial ramifications for an organization. A head-in-the-sand approach to the possibility of cyberthreats is no longer prudent, they say.

Here, Johann Dettweiler, director of operations for Fairfax, Virginia-based compliance management firm TalaTek, talks about the importance of cybersecurity measures and what contractors can do protect themselves.

JOHANN DETTWEILER**:** It's important to note that cybersecurity is important for everyone from Fortune 500 companies to individuals working in a home office. One of the main reasons organizations don't consider cybersecurity is they tend to think of their data as something other than a company asset. Construction companies in particular have a lot of physical assets from materials to vehicles to personnel that something as non-substantive as data can easily be overlooked as an asset to protect.

However, all data is an asset and should be protected. Whether it is the private data of an organization's workforce, such as social security numbers or private human resources (HR) information or the company's proprietary data, such as building plans or construction time frames, if this data were to be exploited, it could have serious legal and/or financial ramifications for an organization.

The idea of cybersecurity is taking the necessary steps and exercising due diligence and care to ensure data that is owned and processed by an organization is considered and necessary steps are taken to ensure some level of protection. The loss of either a client's or employee's sensitive information could result in legal fees and/or punitive damages, as all entities that collect and process this data are required to exercise some form of measures to protect it from unauthorized disclosure. These types of damages are fairly easy to quantify and can hurt an organization's bottom line.

There are also non-quantifiable damages that organizations can suffer, such as loss of client trust and competitive advantage. These types of damages are harder to put a price tag on, but definitely have a substantive impact on an organization's overall profitability.

Do most of them take it seriously?

DETTWEILER**:** It's not that most construction companies don't take cybersecurity seriously. In today's climate, given all of the constant news reports about breaches and data loss, every organization understands the importance of cybersecurity. However, cybersecurity is difficult and it adds to the cost of running an operation.

Most construction firms are so focused on the bottom line and the physical deliverables that many aren't even aware of the various types of sensitive data they possess. A lot of leaders don't understand their data has worth because its intangible and it doesn't have a direct impact on a company's profitability until there is a breach and then it may be too late to think about cybersecurity.

Read the rest here:

https://www.constructiondive.com/news/cybersecurity-expert-all-construction-data-is-an-asset-and-should-be-prot/573037/

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

ISSA-COS 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 external organizations

Cyber Focus Day Symposium – 7th Annual

The Cyber Focus Day Symposium is an annual 2-day event held on the beautiful campus of the University of Colorado Colorado Springs (UCCS). It attracts over 300 attendees from across the nation. This event kicks off with a full day of Capture-the-Flag (CTF) fun and competition. A morning CTF prep session designed to educate beginners is then followed by the actual competition in the afternoon. Lunch is provided and snacks are served throughout the day.

The following day includes a series of keynote speakers, panel discussions, breakout sessions, and an exhibitor hall. Community representatives from partnering organizations are on hand to educate and inform attendees on events coming up within the community. Each annual Cyber Focus Day Symposium emphasizes a theme that guest speakers weave into their presentations.

Highlights for this event include:

- Nationally recognized Keynote Speakers and Large Corporate Sponsors/Exhibitors
- Up to 16 potential Continuing Professional Educations (CPE) Credits Available
- Over 40 Capture-the-Flag participants - all skill levels are welcome – *beginners too!*
- Over $6,000 in prizes and giveaways
- 20 Exhibitor Booths with Live Demos
- Free parking, Free breakfast, Free lunch, and Free afternoon snacks.

March 25 – 26, 2020
UCCS Campus
Register at:
www.issa-cos.org
info@issa-cos.org

Join ISSA-COS on Social Media

Twitter:
- Colorado Springs ISSA
- @COSISSA

LinkedIn:
- ISSA Colorado Springs Chapter
- https://www.linkedin.com/groups/1878203/

Facebook:
- Colorado Springs Chapter of the ISSA
- @ColoradoSpringsISSA

2019 Chapter Sponsors

2020 Chapter Sponsors

MURRAY SECURITY SERVICES

NATIONAL CYBERSECURITY CENTER

L3HARRIS FAST. FORWARD.

UCCS

PIKES PEAK COMMUNITY COLLEGE

Colorado Technical University

Become a 2020 Sponsor Today!

ISSA-COS Community Partners

MURRAY SECURITY SERVICES

NATIONAL CYBERSECURITY CENTER

Colorado SBDC TECHSOURCE

COLORADO SPRINGS

WiCyS

Colorado Springs Chamber & EDC

PIKES PEAK COMMUNITY COLLEGE

Colorado Technical University

U.S. AIR FORCE ACADEMY

CSBJ

COLLEGEAMERICA Since 1994

FOX21 NEWS

BLOCKFRAME

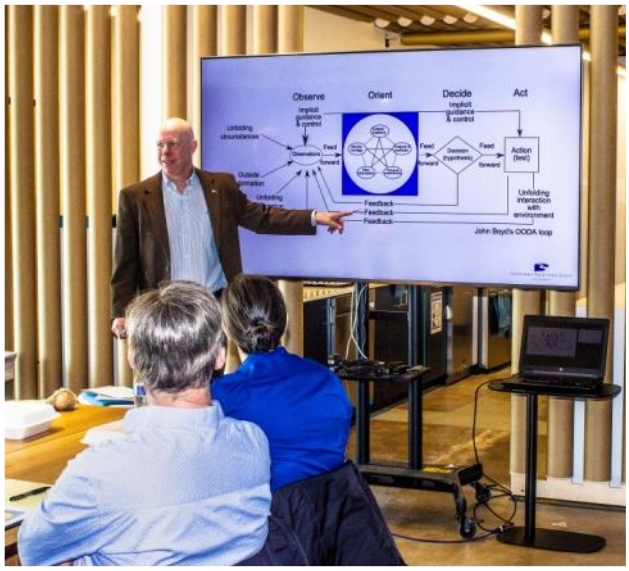
COLORADO PTAC

HANDSHAKE

UCCS

Pikes Peak Business & Education Alliance


ISSA Photos are courtesy of our Chapter Photographer
Reg. No. 35
Warren
Pearce



Additional photographs are available on the ISSA-COS.ORG *website.*

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: Pat Laverty
Past President: Cindy Thornburg
Past President: Frank Gearhart
Past President: Colleen Murphy

This App Automatically Cancels *and Sues* Robocallers

By Edward Ongweso, Jr, Vice, February 12, 2020

DoNotPay, the family of consumer advocacy services meant to protect people from corporate exploitation, is launching a new app aimed at helping end our long national nightmare surrounding robocalls by giving you a burner credit card to get their contact details then giving you a chatbot lawyer to automatically sue them.

Read the rest here:

https://www.vice.com/en_us/article/4agak3/this-app-automatically-cancels-and-sues-roboallers

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