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

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 7 NUMBER 12

DECEMBER 2018

Elections are Coming II

A Note From Our President

By Ms. Colleen Murphy

Colleagues,

As I write this, our annual elections are in progress and my term as President is coming to an end. It has been an honor serving as the President of the Colorado Springs Chapter. We have a truly exceptional chapter, one that offers more to our members – for FREE – than any other ISSA Chapter in the world. Our volunteers do an amazing job planning, organizing, and executing numerous events, providing opportunities for members to earn approximately 60 continuing education credits every year! Our committees consistently work behind-the-scenes providing mentoring services, supporting training events, handling our IT requirements, conducting our elections and our annual audit, and much more. Their engagement is what makes this chapter so special. I'm extremely grateful to every volunteer for their continued support. THANK YOU!

I will continue to support our chapter when and where I can best help. I hope to see many of you at our Annual Awards Luncheon on 6 December and throughout our events next year.

Thank you all for your continued engagement and support of our Chapter!

Colleen

The ISSA Colorado Springs Newsletter incorporates open source news articles in compliance with USC Title 17, Section 107, Paragraph a (slightly truncated to avoid copyright infringement) as a training method to educate readers on security matters .

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our members, and do not constitute or imply endorsement by ISSA or the Colorado Springs Chapter of ISSA of any entity, event, product, service, or enterprise.

The rare form of machine learning that can spot hackers who have already broken in

By Thomas Claburn, The Register, October 15, 2018

In 2013, a group of British intelligence agents noticed something odd. While most efforts to secure digital infrastructure were fixated on blocking bad guys from getting in, few focused on the reverse: stopping them from leaking information out. Based on that idea, the group founded a new cybersecurity company called Darktrace.

The firm partnered with mathematicians at the University of Cambridge to develop a tool that would use machine learning to catch internal breaches. Rather than train the algorithms on historical examples of attacks, however, they needed a way for the system to recognize new instances of anomalous behavior. They turned to unsupervised learning, a technique based on a rare type of machine-learning algorithm that doesn't require humans to specify what to look for.

> *"Most attacks still involve violations of data, privacy, and confidentiality. But we're entering a new era."*

"It's very much like the human body's own immune system," says the company's co-CEO Nicole Eagan. "As complex as it is, it has this innate sense of what's self and not self. And when it finds something that doesn't belong—that's not self—it has an extremely precise and rapid response."

The vast majority of machine-learning applications rely on supervised learning. This involves feeding a machine massive amounts of carefully labeled data to train it to recognize a narrowly defined pattern. Say you want your machine to recognize golden retrievers. You feed it hundreds or thousands of images of golden retrievers and of things that are not, all the while telling it explicitly which ones are which. Eventually, you end up with a pretty decent golden-retriever-spotting machine.

In cybersecurity, supervised learning works pretty well. You train a machine on the different kinds of threats your system has faced before, and it chases after them relentlessly.

But there are two main problems. For one, it only works with known threats; unknown threats still sneak in under the radar. For another, supervised-learning algorithms work best with balanced data sets—in other words, ones that have an equal number of examples of what it's looking for and what it can ignore. Cybersecurity data is highly unbalanced: there are very few examples of threatening behavior buried in an overwhelming amount of normal behavior.

Fortunately, where supervised learning falters, unsupervised learning excels. The latter can look at massive amounts of unlabeled data and find the pieces that don't follow the typical pattern. As a result, it can surface threats that a system has never seen before and needs few anomalous data points to do so.

When Darktrace deploys its software, it sets up physical and digital sensors around the client's network to map out its activity. That raw data is funneled to over 60 different unsupervised-learning algorithms that compete with one another to find anomalous behavior.

Those algorithms then spit their output into yet another master algorithm that uses various statistical methods to determine which of the 60 to listen to and which of them to ignore. All that complexity is packaged into a final visualization that allows human operators to quickly see and respond to likely breaches. As the humans work out what to do next, the system works to quarantine the breach until it's resolved—by cutting off all external communication from the infected device, for example.

Unsupervised learning is no silver bullet, however. As attackers get more and more sophisticated, they get better at fooling machines, whatever type of machine learning they are using. "There is this cat-and-mouse game where attackers can try to change their behavior," says Dawn Song, a cybersecurity and machine-learning expert at the University of California, Berkeley.

Read the rest here:

https://www.technologyreview.com/s/612427/the-rare-form-of-machine-learning-that-can-spot-hackers-who-have-already-broken-in/

Membership Corner

Membership Update

Hottest item! Melissa Absher has decided to give up her position as chairperson for the Mentorship Committee after four years of service in that role. So, we need a volunteer to take on this role for the chapter. If you're interested, please contact me at membership@issa-cos.org or any board member at cos-board-new@issa-cos.org. If you have questions about what the role requires, Melissa can answer any questions you might have—you can reach her at the membership email address above. She will be continuing in her role as Deputy Membership VP.

Watch for all the upcoming activities after the start of the year as we get back into our monthly meetings, mini-seminars and other training. 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.

New Members November
Carissa Nichols
Katie Martin
Shawn Dannen

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.

Our membership stands at ~462 members as of the end of November. As you're going about your daily activities, please take the time to engage your colleagues, ask if they're ISSA members, and if not take a couple of minutes to convince them of the value of becoming a member of our chapter. Word of mouth is our primary method of advertising. If you don't take the time to tell people of our organization, folks won't know all the advantages we bring to their professional life. Renewals are also critical to maintaining our membership. If you are considering not renewing, please talk to me or one of the other board members to help us understand what we can do better to support our membership and retain you as active chapter members.

Thanks,

David Reed

Membership Committee Chairman
dreed54321@comcast.net

Candidates for the Upcoming Chapter Elections

Ernest Campos —Candidate for President

For the last 12-years, I have volunteered as a 1-on-1 professional mentor and have assisted with founding two separate mentoring programs for Non-Profit Organizations (ISSA-COS and George Washington University (GWU) Tech Alumni Association). I currently serve on the Board of Directors for ISSA-COS as the member-elect Vice-President and am often asked to provide insights pertaining to requisite elements needed to maintain a vibrant and sustainable Cybersecurity ecosystem at the individual, organizational, and industry levels. Numerous collegiate institutions, professional organizations, and local government offices throughout Colorado Springs have requested my participation on cyber-related focus groups, round table meetings, and panel discussions.

I have spent nearly thirty (30) years as a Small Business Entrepreneur, First-line Corporate Manager, Senior Program/Project Manager, and an Information Systems Technologist specializing in Complex Computing Solutions. Throughout my career, I have supported numerous Federal organizations including: The White House, The Central Intelligence Agency, The National Reconnaissance Office, The National Counter-Terrorism Center, The Federal Bureau of Investigation, The Department of Homeland Security, The Department of State, and others. Prior to joining industry, I served 11-years in the U.S. Air Force as a White House Communications, Senior Information Systems Technology Lead.

If elected President, my focus will be to elevate current programming for ISSA-COS events while streamlining the effort required to produce our events. I believe more members would volunteer to support our organization if tasks were simplified and well defined. I also plan to expand our footprint into industries beyond just Federal/DoD. As a volunteer to the COS Chamber and EDC, I have gained insight into the needs of other industries such as Healthcare, Finance, and Retail. All of these industries are desperately requesting Cybersecurity guidance and knowledge and we, as members of our own community, depend on their ability to function with security, reliability, an integrity. Last of all, I intend to honor the many years of success ISSA-COS has experience. I won't fix things that aren't broken, and I will uphold our sound reputation.

Jeff Tomkiewicz —Candidate for ISSA-COS Vice President of Training

I'd like the opportunity to serve as your Vice President of Training for the upcoming term of office. Here are my relevant qualifications:

- Member of the Colorado Springs Chapter ISSA since 2017
- 18 year Air Force career with experience in training, course development and management.
- Served various board positions for many professional organizations throughout my career · Bachelor's degree in Cyber Security, University of Maryland University College
- Currently hold Security + and CEH certifications

If elected, I can help the ISSA-COS board succeed in its goals to help the further members professional needs. A few items of interest in my agenda include:

- Create more hands on training opportunities during mini seminars.
- Implement an ISSA Capture the Flag event for all levels.
- Create long-term planning/annual training plan.

Please consider my interest to serve the chapter membership and help further the chapter's success into the future.

Katie Martin—Candidate for Director of Professional Outreach

As a previous student member of the ISSA-COS chapter, I am now a General member and running for the position of Director of Professional Outreach for the next ISSA-COS chapter election.

My career qualifications include over 18 years with Hewlett-Packard (HP) as product marketing manager of many HP product lines including DeskJet printers, Photo printers, All-in-One printers and the Toner business. During my time at HP, I attended the University of Denver and received my MBA in 2002. Innate to my responsibilities with HP were sales force training, presentation of quarterly business updates, managing profit and revenue as well as developing new business opportunities.

After taking a voluntary severance in 2016, I went back to school to learn cybersecurity. I attended SecureSet Academy, was awarded a Google scholarship for further training and passed my CompTIA Security+ cyber certification this summer.

(Continued on page 5)

Some additional volunteer experiences include serving as:

- A fellow with the National Cybersecurity Center (NCC) this summer, helping in their efforts to drive memberships and sponsorships as well as K-12 education and outreach.
- An elected member (1 of 5) of my community's HOA, governing over 1,400 residents.
- A parent advocate and member of Academy School District 20's Food Allergy Task Force.

I would very much appreciate your consideration and vote. I am outspoken and passionate about the need for women in cybersecurity, development of synergistic and strategic partnerships with sister organizations and driving awareness of ISSA-COS's efforts to educate and grow the cybersecurity workforce.

Russ Weeks—Candidate for ISSA-COS Recorder and Historian

I'd like the opportunity to serve as your Recorder and Historian for the upcoming term of office.

Here are my relevant qualifications:

- Member of the Colorado Springs Chapter ISSA since 2012
- Selected as ISSA Senior Member 2018
- Employed by US Air Force as the Academy's Chief Data Officer
- 22 year Air Force career with experience as a network manager
- Bachelor's degree in Information System Management, University of Maryland
- Certified as a CISSP since 2009

I'd like to serve so I can help the ISSA-COS board succeed in its goals to help the members. My agenda includes:

- Record and keep minutes of all meetings, and maintain the official records of the
- Chapter.
- Ensure chapter members are recognized for senior member and fellow status, and for
- submitting members/the chapter for awards.
- Serve as the chapter historian – create the long-term archiving solution for records

Please consider my interest to serve the chapter membership and help with our bright future.

William (Bill) Blake - Candidate for Member-at-Large

I'm running for election to a 2 year term as Member-at-Large this year. I've been a member of the Colorado Springs ISSA chapter since 1998. I've been working in IT and Cyber Security for over 45 years. That includes an even mix of DoD (I'm retired AF) and commercial experience. I've enjoyed being on the board supporting the chapter for the past 2 years and would appreciate your consideration for another 2 years.

Cisco Accidentally Released Dirty Cow Exploit Code in Software

By Lindsey O'Donnell, Threat Post November 8, 2018

Cisco Systems revealed in a security bulletin Wednesday that it "inadvertently" shipped in-house exploit code that was used in security tests of scripts as part of its TelePresence Video Communication Server and Expressway Series software. The code exploits the Dirty Cow vulnerability (CVE-2016-5195), a well-known privilege escalation vulnerability in the Linux Kernel, which came to light in 2016.

The code was used internally by Cisco in validation scripts to be included in shipping software images – it was used to ensure that Cisco's software is protected against known exploits. However, there was a failure in the final QA validation step of the software, and as a result someone from Cisco forgot to remove the code before release.

"The presence of the sample, dormant exploit code does not represent nor allow an exploitable vulnerability on the product, nor does it present a risk to the product itself as all of the required patches for this vulnerability have been integrated into all shipping software images," Cisco wrote in its advisory.

The blunder was discovered during internal security testing.

"A failure in the final QA validation step of the automated software build system for the Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) software inadvertently allowed a set of sample, dormant exploit code used internally by Cisco in validation scripts to be included in shipping software images," the company said in an advisory. "This includes an exploit for the Dirty CoW vulnerability (CVE-2016-5195). The purpose of this QA validation step is to make sure the Cisco product contains the required fixes for this vulnerability."

Read the rest here:

https://threatpost.com/cisco-accidentally-released-dirty-cow-exploit-code-in-software/138888/

Zero-day in popular WordPress plugin exploited in the wild to take over sites

By Catalin Cimpanu, ZDNet, November 9, 2018

Hackers have exploited --and are currently continuing to exploit-- a now-patched zero-day vulnerability in a popular WordPress plugin to install backdoors and take over sites.

The vulnerability affects WP GDPR Compliance, a WordPress plugin that helps site owners become GDPR compliant. The plugin is one of the most popular GDPR-themed plugins on the WordPress Plugins directory, with over 100,000 active installs.

Around three weeks ago, attackers seem to have discovered a vulnerability in this plugin and began using it to gain access to WordPress sites and install backdoor scripts.

Initial reports about hacked sites were made into another plugin's support forum, but that plugin turned out to have been installed as a second-stage payload on some of the hacked sites.

After investigations led by the WordPress security team, the source of the hacks was eventually traced back to WP GDPR Compliance, which was the common plugin installed on all reported compromised sites.

The WordPress team removed the plugin from the official Plugins directory earlier this week after they identified several security issues within its code, which they believed were the cause of the reported hacks.

The plugin was reinstated two days ago, but only after its authors released version 1.4.3, which contained patches for the reported issues.

But despite the fixes, attacks on sites still running versions 1.4.2 and older are still going on, according to security experts from Defiant, a company that runs the Wordfence firewall plugin for WordPress sites.

The company's analysts say they're continuing to detect attacks that try to exploit one of the reported WP GDPR Compliance security issues.

In particular, attackers are targeting a WP GDPR Compliance bug that allows them to make a call to one of the plugin's internal functions and change settings for both the plugin, but also for the entire WordPress CMS.

The Wordfence team says they've seen two types of attacks using this bug. The first scenario goes like this:

- Hackers use bug to open the site's user registration system.
- Hackers use bug to set the default role for new accounts to "administrator."
- Hackers register a new account, which automatically becomes an administrator. This new account is usually named "t2trollherten."
- Hackers set back default user role for new accounts to "subscriber."
- Hackers disable public user registration.
- Hackers log into their new admin account.

They then proceed to install a backdoor on the site, as a file named wp-cache.php.

Read the rest here:

https://www.zdnet.com/article/zero-day-in-popular-wordpress-plugin-exploited-in-the-wild-to-take-over-sites/

Hacker backdoors popular JavaScript library to steal Bitcoin funds

By Catalin Cimpanu, ZDNet, November 26, 2018

A hacker has gained (legitimate) access to a popular JavaScript library and has injected malicious code that steals Bitcoin and Bitcoin Cash funds stored inside BitPay's Copay wallet apps.

The presence of this malicious code was identified last week, but only today have researchers been able to understand what the heavily obfuscated malicious code actually does.

The library loading the malicious code is named Event-Stream, a JavaScript npm package for working with Node.js streaming data.

This is an extremely popular JavaScript library, with over two million weekly downloads on the npmjs.com repository, but about three months ago, its original author, due to a lack of time and interest, handed its development over to another programmer named Right9ctrl.

But according to an eagle-eyed user who spotted issues with Event-Stream last week, Right9ctrl had immediately poisoned the library with malicious code.

Right9ctrl released Event-Stream 3.3.6 which contained a new dependency --for the Flatmap-Stream library version 0.1.1. The Flatmap-Stream library v0.1.1 is where the malicious code resides.

According to users on Twitter, GitHub, and Hacker News, this malicious code lays dormant until it's used inside the source code of Copay, a desktop and mobile wallet app developed by Bitcoin payment platform BitPay.

Once the malicious code has been compiled and shipped inside poisoned versions of the Copay wallet app, it will steal users' wallet information, including private keys, and send it to the *copayapi.host* URL on port *8080*.

It is believed that the hacker is using this information to empty victims' wallets. In a blog post, the Copay team said all versions between 5.0.1 and 5.1.0 were officially deemed infected, and urged users to update to version 5.2.0 or later.

Maintainers of the npmjs.com JavaScript package repository have also intervened and taken down the Flatmap-Stream library from their site, making it inaccessible to all the projects where this was being loaded via the npm package installer utility.

The malicious Event-Stream v3.3.6 has also been taken down from npmjs.com, but the Event-Stream library is still available. This is because Right9ctrl, in an attempt to hide his malicious code, released subsequent versions of Event-Stream that didn't contain any malicious code.

Project maintainers who use these two libraries are advised to update their dependency trees to the latest version available --Event-Stream version 4.0.1. This link contains a list of all the 3,900+ JavaScript npm packages where Event-Stream is loaded as a direct or indirect dependency.

This manual update/removal step is necessary as some projects are configured to cache all dependencies locally, and might not trigger the usual console error when attempting to download a non-existent npm package from npmjs.com when building a new project version.

This is not the first JavaScript/npm-related security issue that has taken place in the past years. In July this year, a hacker compromised the ESLint library with malicious code that was designed to steal the npm credentials of other developers.

In May 2018, a hacker tried to hide a backdoor in another popular npm package named getcookies.

Read the rest here:

https://www.zdnet.com/article/hacker-backdoors-popular-javascript-library-to-steal-bitcoin-funds/

Increasing Risk of Cyber Attacks During Holidays Says Report

By Sergiu Gatlan, Softpaedia, November 26, 2018

Organizations and individuals are at a higher risk of experiencing a cyber attack during the holidays, starting with Black Friday and ending with Christmas, according to a report from Carbon Black's Threat Analysis Unit (TAU).

As detailed in TAU's 2018 Carbon Black Holiday Threat Report, cyberattacks usually see a substantial increase in frequency during the winter holidays, with the trends going up for the past two years right before Black Friday and reaching the highest spikes during the days following Christmas.

After analyzing more than 16 million endpoints, TAU observed that during the 2016 holiday season organization experienced an increase in the number of cyber attacks of 20,5% above the normal levels.

Furthermore, during the holiday season of 2017, the attempted number of attacks against the endpoints monitored by Carbon Black saw a 57,5% accretion rate.

“Based on existing precedent, we expect the same trend to continue, if not increase, during the 2018 holiday shopping season,” said Tom Kellermann, Carbon Black’s Chief Cybersecurity Officer. “During the holiday season, there is often a ton of noise in the online world and attackers do everything they can to take advantage of that."

Understaffed companies are most vulnerable during holidays

Kellerman also stated that the increase in cyber attack rates for the holiday season applies to both organizations and individuals, all of them being at a higher risk of having their data compromised.

TAU's report says that the vast majority of cyber attacks that happen during the holidays use phishing campaigns or spear-phishing campaigns to deliver malware payloads designed to compromise the victim's computing systems.

Following this type of "holiday-themed" cyber attacks that targeted major retailers were able to successfully breach their IT systems and compromise the personal and financial information of millions of customers.

Read the rest here:

https://news.softpedia.com/news/increasing-risk-of-cyber-attacks-during-holidays-says-report-523989.shtml

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.

Get Your Chapter Of The Year - 2017 Shirt NOW!

Our apologies for the delay in getting the Chapter of the Year shirt ordering information out to everyone.

We won this prestigious award because of your hard work, dedication, and exceptional support of our Chapter. Chapter of the Year recognition is difficult to achieve as there is strong competition among all ISSA chapters worldwide. We should be very proud of earning this prestigious honor. To enable everyone to show our accomplishment, we worked with a local shirt company to provide two options for a Chapter of the Year shirt.

Here is a summary of the Chapter of the Year shirt info:

TYPES:

- Long-sleeve button up
- Short-sleeve Polo

COLOR:

- Navy Blue

SIZE:

- Mens and Ladies sizes: S, M, L, XL, XXL

ORDERS:

- Place your order and pay via the Eventbrite links below

COST:

- Long-sleeve button up: $35.00 ($2.00 more for XXL)
- Short-sleeve Polo: $28.50 ($2.00 more for XXL)

ISSA

Chapter of the Year 2017

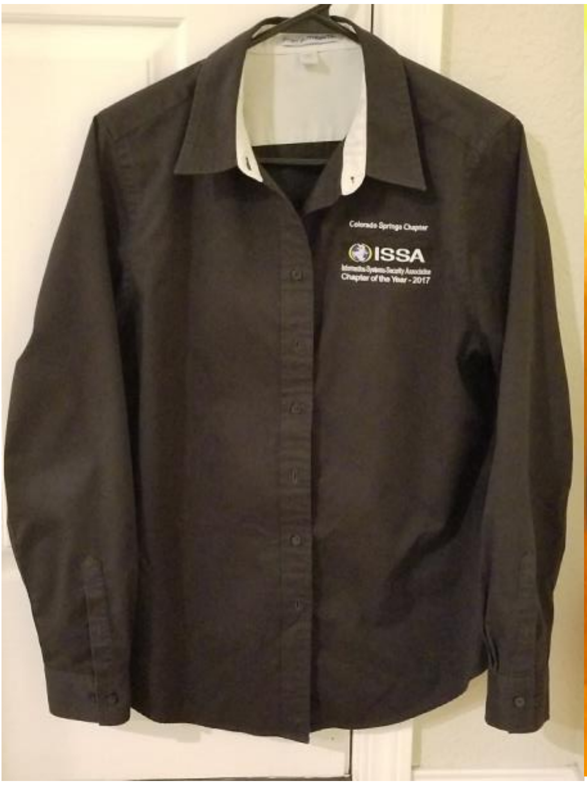
PICK UP YOUR SHIRT AT A CHAPTER LUNCH OR DINNER MEETING

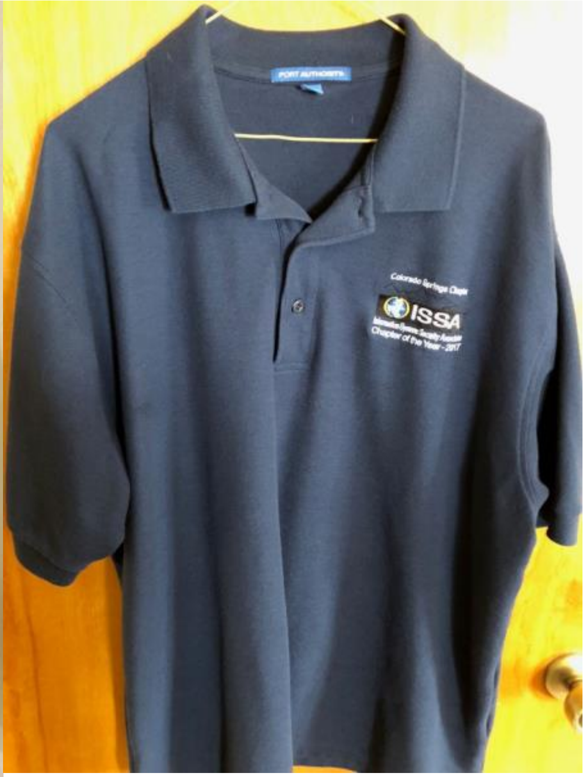
If you have any questions or special requests, please send an email to member-at-large@issa-cos.org.

Select the shirt you want via the following two Eventbrite links. Select the size you want after you select the type of shirt.

https://www.eventbrite.com/e/issa-cos-shirts-long-sleeve-button-down-shirt-tickets-49269320865

https://www.eventbrite.com/e/issa-cos-shirts-short-sleeve-polo-shirt-tickets-48316223124


Colorado Springs Chapter
ISSA
Information Systems Security Association
Chapter of the Year - 2017


Colorado Springs Chapter
ISSA
Information Systems Security Association
Chapter of the Year - 2017

Iran’s ‘cyber attacks’ against US can cause damage, experts warn

By Staff Writer, Al Arabiya English, November 22, 2018

As the United States completes its withdrawal from the Iran nuclear agreement, security analysts warn of more frequent and dangerous cyber attacks from Iran.

The president of the Global Situation Room, Inc. and the former White House director of Global Engagement, Brett Bruen warned that: “We are very likely to see Tehran in the coming days and weeks target American interests.”

He added that: “The most vulnerable and important objective for them are American businesses. They see effecting some economic impact as retribution.”

The United States fully re-imposed sanctions on Iran on November 5.

For their part, a recent report from the Foundation for Defense of Democracies (FDD) said that: “The desperate regime may become a more aggressive actor both in the virtual and physical world … its hackers can still do serious damage,” according to a report on Fox news.

Analysts also said Iran’s capabilities are evolving and focusing more on using social media to spread false information and skew public opinion.

Bruen said that: “Some of those efforts were identified and taken down by social media companies. Many have not been detected or removed. The most damaging, as we saw with Russia, is when a country can penetrate networks and then weaponize that information.”

In August, US intelligence experts warned that the United States is preparing to brace itself against cyber attacks which Iran might launch in response to the restoring of US sanctions in early November.

While the Iranians showed more defiance with the Iranian Supreme Leader Ayatollah Ali Khamenei calling in late October for the stepping up of efforts to fight enemy “infiltration” in a speech to officials in charge of cyber defense, state television reported.

Read the rest here:

http://english.alarabiya.net/en/News/middle-east/2018/11/22/Iran-s-cyber-attacks-against-US-can-pose-damage-experts-warn.html?utm_source=360Works%20CloudMail&utm_medium=email&utm_campaign=NewsWatch

Update Your Profile!

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

DHS Cybersecurity Branch Signed into Existence by Trump

By Sergiu Gatlan, Softpaedia, November 16, 2018

Donald Trump, the President of U.S., signed today the Cybersecurity and Infrastructure Security Agency Act of 2018 which officializes the new cybersecurity branch of the Department of Homeland Security (DHS).

"CISA's responsibilities include: leading cybersecurity and critical infrastructure security programs, operations, and associated policy; coordinating with non-federal and federal entities; and carrying out DHS's responsibilities concerning chemical facility antiterrorism standards," says the summary of the bill signed by Trump on November 16.

Moreover, CISA encompasses multiple divisions which were formerly part of the DHS, namely the Infrastructure Security Division, the Cybersecurity Division, and the Emergency Communications Division.

Through the bill POTUS signed on November 16, the former DHS main cybersecurity named National Protection and Programs Directorate (NPPD) is rebranded as the Cybersecurity and Infrastructure Protection Agency.

Christopher Krebs, NPPD undersecretary and most probably the future director of the CISA agency said that "The CISA Act passing Congress represents real progress in the national effort to improve our collective efforts in cybersecurity."

The CISA Act was unanimously voted by the House of Representatives on November 13

In addition, according to Krebs, the new Cybersecurity and Infrastructure Security Agency also has a mission the streamlining of DHS cybersecurity operations, as well as improve the security of critical U.S. infrastructure and cyber platforms.

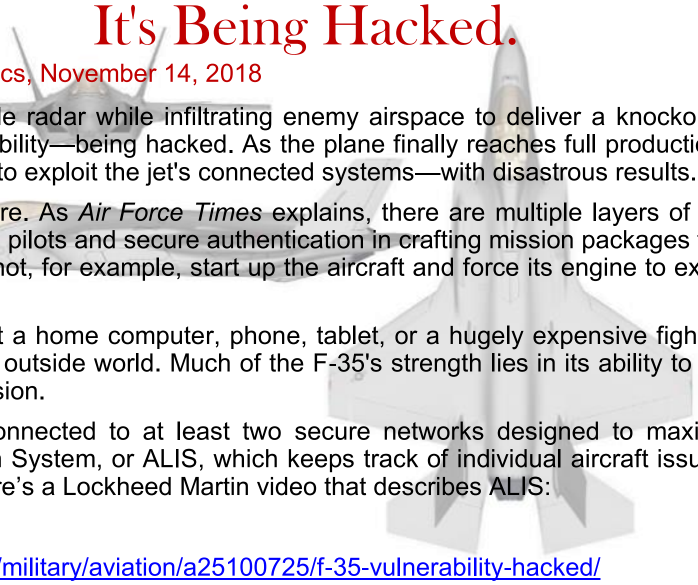
The CISA was created as the Federal leading agency which will take on all matters regarding cyber and physical infrastructure security.

Read the rest here:

https://news.softpedia.com/news/dhs-cybersecurity-branch-signed-into-existence-by-trump-523832.shtml

The F-35's Greatest Vulnerability Isn't Enemy Weapons. It's Being Hacked.

By Kyle Mizokami, Popular Mechanics, November 14, 2018



The F-35 Lightning II can evade radar while infiltrating enemy airspace to deliver a knockout blow. It's a sophisticated, stealthy fighter with one big vulnerability—being hacked. As the plane finally reaches full production, the Air Force is racing to plug holes that could allow hackers to exploit the jet's connected systems—with disastrous results.

The aircraft itself is pretty secure. As *Air Force Times* explains, there are multiple layers of security surrounding the jet, including PIN numbers for individual pilots and secure authentication in crafting mission packages for uploading into the aircraft computer. A faraway hacker could not, for example, start up the aircraft and force its engine to explode, or cause the airplane to roll off the runway and crash.

But whether we're talking about a home computer, phone, tablet, or a hugely expensive fighter jet, vulnerabilities add up the more you're connected with the outside world. Much of the F-35's strength lies in its ability to connect to the wider military and harness big data about the mission.

The worldwide F-35 fleet is connected to at least two secure networks designed to maximize efficiency. The first is the Autonomic Logistics Information System, or ALIS, which keeps track of individual aircraft issues and the location of spare parts and equipment worldwide. Here's a Lockheed Martin video that describes ALIS:

Read the rest here:

https://www.popularmechanics.com/military/aviation/a25100725/f-35-vulnerability-hacked/

Upstream devoted to truck cybersecurity threats

By Matthew Borst, SAW, August 7, 2018

Automation is about more than just turning simple human actions into machine processes. Because I spend my time working with organizations on security orchestration, automation, and response (SOAR) solutions that apply automation across many aspects of the incident response and case management lifecycle, I have a unique perspective on the variety of ways that organizations can get value from investing in automated tools.

According to Gartner, Inc, a leading research and advisory company, the number of connected vehicles on the road is expected to reach 250 million by 2020. The heavy-duty industry has seen connectivity grow inside the truck with fleet monitoring telematics, real-time navigation, and electronic logging devices (ELDs). However, questions continue to remain over the security of these new technologies and the vulnerabilities created on these vehicles. Upstream Security has developed a cloud-based cybersecurity platform to address truck security immediately.

“There are 100 million vehicles on the road today with some level of connectivity,” Jeff Lebowitz, VP of Market Development at Upstream, told *Truck and Off-Highway Engineering*. “So, to me, the biggest need in the industry is acceptance and understanding of the risk today, how it’s going to dramatically increase in two years when there’s 200 million vehicles connected, and what does that really mean?”

Manufacturers and fleet operators recognize the risk that is inherent to having connected trucks transmitting navigation, powertrain, and other pertinent information between the vehicle and specified networks. Some companies have approached the security of the vehicle with physical devices on the truck that act like local firewalls such as what personal computers use. However, these devices are still being developed to the level that is required to fully secure vehicles.

Upstream is leveraging its cloud-based platform to protect trucks now. The system is referred to as Upstream Security C4 (Centralized Connected Car Cybersecurity) Platform and was purpose-built to handle the big data developed by connected trucks, including telematics, mobile data, over-the-air updates, and other data generators. The platform combines four cybersecurity engines working in unison to analyze communications from the protocol level up: protocol security, transactional security, contextual security, and behavioral security.

Since there is no hardware or software on the vehicle, Upstream can monitor communications between data centers and fleets to detect, interpret, and alert them in real-time. The company also plans to implement a layered protection approach to vehicle cybersecurity once those devices finally make their way into production trucks.

Upstream acknowledges that the trucking industry is trying to take steps to mitigate these security issues.

“The most advanced organization is the American Trucking Associations, where they have raised awareness on cyber concerns better than any other organization that I have seen,” Lebowitz said. “In between, you have the telematics service providers who understand that if their servers get hit and there’s a lockdown, that is enormous damage to them. So, I think that is another layer where there are people focused on security.”

Read the rest here:

https://www.sae.org/news/2018/08/upstream-cybersecurity

Vaporworms: New breed of self-propagating fileless malware to emerge in 2019

By Staff, HelpNet Security, November 16, 2018

WatchGuard Technologies' information security predictions for 2019 include the emergence of vaporworms, a new breed of fileless malware with wormlike properties to self-propagate through vulnerable systems, along with a takedown of the internet itself and ransomware targeting utilities and industrial control systems.

"Cyber criminals are continuing to reshape the threat landscape as they update their tactics and escalate their attacks against businesses, governments and even the infrastructure of the internet itself," said Corey Nachreiner, CTO at WatchGuard Technologies. "The Threat Lab's 2019 predictions span from highly likely to audacious, but consistent across all eight is that there's hope for preventing them. Organisations of all sizes need to look ahead at what new threats might be around the corner, prepare for evolving attacks and ensure they're equipped with layered security defences to meet them head-on."

The WatchGuard Threat Lab's 2019 Security Predictions are:

- Vaporworms or Fileless malware worms will emerge

  Fileless malware strains will exhibit wormlike properties in 2019, allowing them to self-propagate by exploiting software vulnerabilities. Fileless malware is more difficult for traditional endpoint detection to identify and block because it runs entirely in memory, without ever dropping a file onto the infected system.

  Combine that trend with the number of systems running unpatched software vulnerable to certain exploits and 2019 will be the year of the vaporworm.

- Attackers hold the Internet hostage

  A hacktivist collective or nation-state will launch a coordinated attack against the infrastructure of the internet in 2019. The protocol that controls the internet (BGP) operates largely on the honour system, and a 2016 DDoS attack against hosting provider Dyn showed that a single attack against a hosting provider or registrar could take down major websites. The bottom line is that the internet itself is ripe for the taking by someone with the resources to DDoS multiple critical points underpinning the internet or abuse the underlying protocols themselves.

- Escalations in State-level cyber attacks force a UN Cyber Security Treaty

  The UN will more forcefully tackle the issue of state-sponsored cyber attacks by enacting a multinational Cyber Security Treaty in 2019.

- AI-Driven chatbots go rogue

  In 2019, cyber criminals and black hat hackers will create malicious chatbots on legitimate sites to socially engineer unknowing victims into clicking malicious links, downloading files containing malware, or sharing private information.

- A major biometric hack will be the beginning of the end for single-factor authentication

  As biometric logins like Apple's Face ID become more common, hackers will take advantage of the false sense of security they encourage and crack a biometric-only login method at scale to pull off a major attack. As a result, 2019 will see strong growth in the use of multi-factor authentication (MFA) for added protection among groups with more security knowledge, particularly push-based authentication and MFA for cloud application defence.

- A nation-state to take 'Fire Sale' attacks from fiction to reality

  In the Die Hard movie series, a 'fire sale' was a fictional three-pronged cyber attack, targeting a city or state's transportation operations, financial systems, public utilities and communication infrastructure. The fear and confusion caused during this attack was designed to allow the terrorists to siphon off huge sums of money undetected. Modern cyber security incidents suggest that nation-states and terrorists have developed these capabilities, so 2019 may be the first year one of these multi-pronged attacks is launched to cover up a hidden operation.

- Hackers to cause real-world blackouts as targeted ransomware focuses on utilities and industrial control systems

Read the rest here:

https://www.helpnetsecurity.com/2018/11/16/self-propagating-fileless-malware/

Despite rise in security awareness, employees' poor security habits are getting worse

By Staff, HelpNet Security, November 14, 2018

Despite an increased focus on cybersecurity awareness in the workplace, employees' poor cybersecurity habits are getting worse, compounded by the speed and complexity of the digital transformation.

Of the 1,600 global employees Vanson Bourne surveyed, 75% of respondents admitted to reusing passwords across accounts, including work and personal.

Organizations are at varying stages of the digital transformation, and that evolution has presented an increasingly complex IT environment to manage securely. Yet the survey findings points to a workforce who are less committed to security best practices. This has not only introduced more risk, but also a sense of frustration between the IT team trying to secure and enable the business and users who want to work more efficiently.

Over half (55%) of survey respondents stated their IT department can be a source of inconvenience in their organization. This leads to employees skirting IT policies, such as the 31% who admitted that they have deployed software without IT's help (i.e. 'shadow IT').

Efforts to get around IT may not necessarily be done with malicious intent, but the reality is they directly increase IT risk for the organization. For example, 13% of employees admitted they would not immediately notify their IT department if they thought they had been hacked.

Further compounding this issue is a workforce that tends not to understand the role of all employees in keeping an organization secure, as 49% of respondents would actually blame the IT department for a cyberattack if one occurred as a result of an employee being hacked.

However, it's not just today's employees exposing organizations to risk. As the digital transformation blurs the traditional security perimeter with cloud apps, it is also redefining the definition of a "user." Enterprises are increasingly adopting software bots powered by robotic process automation (RPA), and granting them access to mission-critical applications and data, like their human counterparts.

Read the rest here:

https://www.helpnetsecurity.com/2018/11/14/poor-security-habits-are-getting-worse/

CYBER ATTACK?!!
ONLINE ELECTION CAMPAIGNING.
DAHL 684
Rogerdahl@aol.com
THE NOT-SO-DISTANT RAUCOUS, MUDSLINGING FUTURE...

New Data Show Demand for Cybersecurity Professionals Accelerating

By Staff, NIST, November 7, 2018

Employer demand for cybersecurity professionals across the United States continues to accelerate, according to new data published today on CyberSeek™, a free online resource from the U.S. Department of Commerce's National Institute of Standards and Technology (NIST), Burning Glass and CompTIA.

U.S. employers in the private and public sectors posted an estimated 313,735 job openings for cybersecurity workers between September 2017 and August 2018. That's in addition to the 715,000-plus cybersecurity workers currently employed around the country.

The new figures from CyberSeek were announced today at the National Initiative for Cybersecurity Education (NICE) Conference in Miami. The NICE program, led by NIST, is a partnership between government, academia and the private sector focused on cybersecurity education, training and workforce development. CyberSeek was created by CompTIA, an IT industry association, and Burning Glass Technologies, an analytics software company, through a grant awarded by NIST in 2015.

The new CyberSeek data show that cybersecurity workers are in particular demand, even as job openings outpace job seekers in the U.S. Across all occupations, there are currently 5.8 employed workers for every job opening. Within the cybersecurity field, the ratio of existing cybersecurity workers to the number of cybersecurity job openings is 2-to-3. That means employers have fewer trained cybersecurity workers in the labor force to choose from and must look to other tactics—including retraining current workers or attracting and training new talent—to fill their needs for cybersecurity professionals.

CyberSeek is aligned with NIST's NICE Cybersecurity Workforce Framework, which categorizes and describes cybersecurity work and helps CyberSeek provide clear data on which job roles are most in demand. The latest CyberSeek update reveals that positions in Operate and Maintain (207,190 openings), Securely Provision (186,864), Protect and Defend (129,716), and Analyze (124,389) are the most sought after by employers.

Among specific core jobs, the top five by employer demand are cybersecurity engineer, cybersecurity analyst, cybersecurity manager/administrator, cybersecurity consultant and penetration and vulnerability tester.

The Washington, D.C., metropolitan area has the largest number of job openings for cybersecurity professionals (44,058). Rounding out the top five metro areas are New York City (20,243), Dallas (12,062), Chicago (11,201) and Los Angeles (10,589).

CyberSeek Career Resources

Beyond the comprehensive supply-and-demand data, CyberSeek also features an interactive career pathway showing key jobs within cybersecurity, common transition opportunities between them and detailed information about the salaries, credentials and skillsets associated with each role.

For example, average salaries for core cybersecurity jobs range from $75,000 for a cybersecurity specialist/technician to $129,000 for a cybersecurity architect.

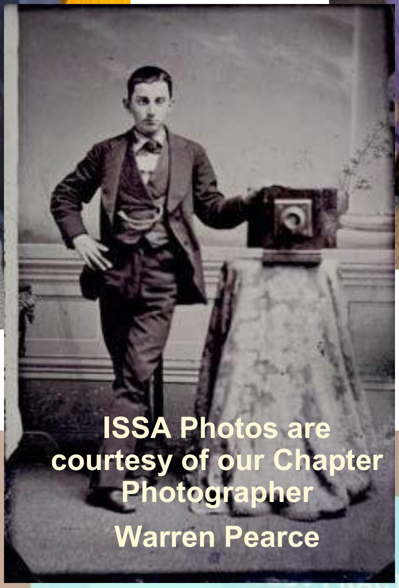
CyberSeek provides content to help local employers, educators, guidance and career counselors, students, current workers, policy makers and other stakeholders build and maintain the U.S. cybersecurity workforce. Visit https://www.cyberseek.org/.

NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life. NIST is a non-regulatory agency of the U.S. Department of Commerce. To learn more about NIST, visit www.nist.gov.

The article may be found here:

https://www.nist.gov/news-events/news/2018/11/new-data-show-demand-cybersecurity-professionals-accelerating

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



ISSA Photos are courtesy of our Chapter Photographer

Warren Pearce

Information Systems Security Association

Developing and Connecting Cybersecurity Leaders Globally

Colorado Springs Chapter

WWW.ISSA-COS.ORG

Chapter Officers:

President:: Colleen Murphy
Executive Vice President: Scott Frisch
Vice President: Ernest Campos
Vice President of Membership: David Reed

- Deputy VP Membership: Melissa Absher

Vice President of Training: Mark Heinrich

- Deputy VP Training: Susan Ross

Treasurer: Mark Maluschka

- Deputy Treasurer: Chuck Wright

Communications Officer: Anna Johnston

- Dep. Communications Officer: Christine Mack

Recorder/Historian: Russ Weeks

- Deputy Recorder/Historian: **Vacant**

Member at Large: James Asimah
Member at Large: **Vacant**
Member at Large: Bill Blake
Member at Large: Jim Blake
Dir. of Certification: Kurt Danis

- Dep Dir Certifications: **Vacant**

Dir. of Professional Outreach: Patrice Siravo

- Dep Dir. of Professional Outreach: June Shores

Committee Chairs:

Ethics: Tim Westland
IT Committee: Patrick Sheehan
Mentorship: Melissa Absher
Recognition: Erik Huffman
Sponsorship: Ernest Campos
Transformation: Ernest Campos
Newsletter: Don Creamer

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?

If you would like to submit an article…

Do you have something that the Colorado Springs ISSA community should know about? Tell us about it!

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

Send your article ideas to *Don Creamer* at:

newsletter@issa-cos.org

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

Past Senior Leadership

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

Real "fake news": China introduces AI news anchor

By Rich Haridy, New Atlas, November 8, 2018

China's state-run news agency, Xinhua, has revealed it will deploy a new digitally generated newsreader to report the news in both Chinese and English languages.

Read the rest here:

https://newatlas.com/china-ai-digital-news-anchor/57158/?utm_medium=email&utm_campaign=2018-11-09%20153244%20USA%20Daily%20Basic%202018-11-09%20153841%20Study%20suggests%20that%20blue%20light%20reduces%20blood%20pressure&utm_content=2018-11-09%20153244%20USA%20Daily%20Basic%202018-11-09%20153841%20Study%20suggests%20that%20blue%20light%20reduces%20blood%20pressure+CID_0b3025ca66cbbccdca4abd1926cf81fd&utm_source=Campaign%20Monitor&utm_term=Read%20more

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