Colorado Springs Chapter ISSA Information Systems Security Association

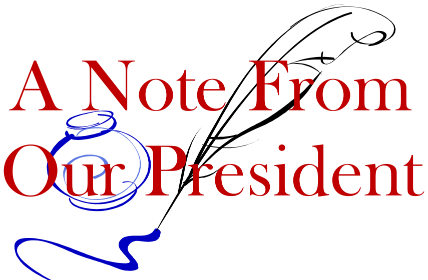
WWW.ISSA-COS.ORG

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 7 NUMBER 2 FEBRARY 2018

Awards Season Is Upon Us



A Note From Our President

By Ms. Colleen Murphy

Colleagues,

ISSA International Fellows Program

The 2018 ISSA International Fellows cycle is open, and applications will be accepted until 23 March. (See Page 6) The Fellows Program recognizes sustained membership and contributions to the profession. 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.

Have you been a member of ISSA for five years? Do you have 10 years of relevant professional experience? If so, you may be eligible to become an ISSA Senior Member.

Have you been a member of ISSA for eight years, and served for three years in a leadership role? Do you have five years of significant performance in the profession such as substantial responsibilities in leading a team or project, performing research with some measure of success, or faculty developing and teaching courses? If so, you may be eligible to become an ISSA Fellow.

If you have 12 years of association membership, 16 years of relevant professional experience, five years of sustained volunteer leadership in the association, and 10 years of documented exceptional service to the security community and a significant contribution to security posture or capability, then you may be eligible to become an ISSA Distinguished Fellow.

These are the general criteria from ISSA International's website to apply for Senior Member, Fellow, or Distinguished Fellow recognition. Don't miss out on getting the professional recognition you've earned. Talk to the Recognition Committee, or any Board member, about how to apply. We'll help you with your submission, endorsement from the Chapter, and for Fellow/Distinguished Fellow candidates, a nomination from a current Fellow or Distinguished Fellow. Application Forms and Fellow Program Guidelines can be found at https://www.issa.org/?page=FellowProgram.

(Continued on page 10)

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.

Uber's Secret Tool for Keeping the Cops in the Dark

By Olivia Zaleski and Eric Newcomer, Bloomberg BusinessWeek, January 11, 2018

In May 2015 about 10 investigators for the Quebec tax authority burst into Uber Technologies Inc.'s office in Montreal. The authorities believed Uber had violated tax laws and had a warrant to collect evidence. Managers on-site knew what to do, say people with knowledge of the event.

Like managers at Uber's hundreds of offices abroad, they'd been trained to page a number that alerted specially trained staff at company headquarters in San Francisco. When the call came in, staffers quickly remotely logged off every computer in the Montreal office, making it practically impossible for the authorities to retrieve the company records they'd obtained a warrant to collect. The investigators left without any evidence.

Most tech companies don't expect police to regularly raid their offices, but Uber isn't most companies. The ride-hailing startup's reputation for flouting local labor laws and taxi rules has made it a favorite target for law enforcement agencies around the world. That's where this remote system, called Ripley, comes in. From spring 2015 until late 2016, Uber routinely used Ripley to thwart police raids in foreign countries, say three people with knowledge of the system. Allusions to its nature can be found in a smattering of court filings, but its details, scope, and origin haven't been previously reported.

"Uber wanted to shield evidence of its illegal activities."

The Uber HQ team overseeing Ripley could remotely change passwords and otherwise lock up data on company-owned smartphones, laptops, and desktops as well as shut down the devices. This routine was initially called the unexpected visitor protocol. Employees aware of its existence eventually took to calling it Ripley, after Sigourney Weaver's flamethrower-wielding hero in the *Alien* movies. The nickname was inspired by a Ripley line in *Aliens*, after the acid-blooded extraterrestrials easily best a squad of ground troops. "Nuke the entire site from orbit. It's the only way to be sure."

Other companies have shut off computers during police raids, then granted officers access after reviewing a warrant. And Uber has reason to be cautious with the sensitive information it holds about customers and their locations around the world. Ripley stands out partly because it was used regularly—at least two dozen times, the people with knowledge of the system say—and partly because some employees involved say they felt the program slowed investigations that were legally sound in the local offices' jurisdictions. "Obstruction of justice definitions vary widely by country," says Ryan Calo, a cyberlaw professor at the University of Washington. "What's clear is that Uber maintained a general pattern of legal arbitrage."

"Like every company with offices around the world, we have security procedures in place to protect corporate and customer data," Uber said in a statement. "When it comes to government investigations, it's our policy to cooperate with all valid searches and requests for data."

Uber has already drawn criminal inquiries from the U.S. Department of Justice for at least five other alleged schemes. In February, the *New York Times* exposed Uber's use of a software tool called Greyball, which showed enforcement officers a fake version of its app to protect drivers from getting ticketed. Ripley's existence gives officials looking into other Uber incidents reason to wonder what they may have missed when their raids were stymied by locked computers or encrypted files. Prosecutors may look at whether Uber obstructed law enforcement in a new light. "It's a fine line," says Albert Gidari, director of privacy at Stanford Law School's Center for Internet & Society. "What is going to determine which side of the line you're on, between obstruction and properly protecting your business, is going to be things like your history, how the government has interacted with you."

About a year after the failed Montreal raid, the judge in the Quebec tax authority's lawsuit against Uber wrote that "Uber wanted to shield evidence of its illegal activities" and that the company's actions in the raid reflected "all the characteristics of an attempt to obstruct justice." Uber told the court it never deleted its files. It cooperated with a second search warrant that explicitly covered the files and agreed to collect provincial taxes for each ride.

Read the rest here:

https://www.bloomberg.com/news/articles/2018-01-11/uber-s-secret-tool-for-keeping-the-cops-in-the-dark

Membership Corner

Membership Update

New Members January
Sheryl Johnson
Sean Campbell
Kenneth Collette
Jareh Dalke
Jose Puello Santana
Peter Farrell
John Vorhees
Peter Granger Jr.

First, 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 holding steady at ~489 members as of the end of January. We're actively developing activities for the upcoming year that should keep the membership engaged—a new approach to the March Cyber Focus Day, new venues for activities, etc. Please watch the Newsletter, communications and eVites to ensure you stay aware of what's going on in the chapter. Please continue to refer new members to the chapter. Referrals are a critical part of developing new members for ISSA. As always, if you have any membership questions don't hesitate to contact me.

Thanks,

David Reed

Membership Committee Chairman

dreed54321@comcast.net

Training News

The ISSA COS Mini-seminars for 2018 kick off Saturday, February 17, with the timely and curious topic "Blockchain Technology: What is it and why is it important?" Our own Srikant Mantravadi and Chris Gorog will team up to show us the basic technology (Srikant) and its financial, social, and economic possibilities (Chris). This promises to be a great start to our series. Invitations will go out soon.

Congratulations are due to Susan Ross and her intrepid team of reviewers and writers who are updating the Security+ materials. CompTIA has updated the exam and we will be ready for our pre-exam review sessions later this year.

I look forward to seeing all of you in the coming weeks.

If you have any questions, contact our Training Committee leads at:Training@ISSA-COS.org.

Mark Heinrich

CISSP, VP Training

Fundamentals of Cybersecurity Camp

University of CINCINNATI

School of Information Technology

Join us in learning Key Cybersecurity Skills

The shortfall of cybersecurity talent working in the federal government poses an imminent national security risk. Through the Fundamentals of Cybersecurity program, the University of Cincinnati, in partnership with Discovery Lab Global and HumanIT, will train you to find a place in this critical need area.

discoverylabglobal.com

humanit.us

The US Bureau Labor Statistics (BLS) projects cybersecurity jobs to increase 18% through 2024, twice the average for all occupations. These jobs are high paying -- the median annual salary for cybersecurity analyst in 2016 was $92,600 (BLS).

Benefits of attending this government funded training program:

- No cost, no risk, online part-time Virtual Reality camp
- Work one-on-one with mentors to receive 3 college credits
- Scholarships available if you plan to continue in a degree or certificate program

Whether you are already in a government position, a veteran, or in another public service area, this program provides accessibility for all, and is a great opportunity to merge your service experience into the cybersecurity field to enhance or start a new career with the government or private sector.

This free **12-week** camp can lead to our cybersecurity certificate at UC, or you can begin an associates in cybersecurity from our two community college partners to prepare you for a job in cybersecurity.

CLARK STATE COMMUNITY COLLEGE

SINCLAIR COLLEGE

Community college partners

This program is designed for:

- Current government employees
- Veterans and active militaty
- Public service employees

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

Application Due:

February 16, 2018

Class Starts:

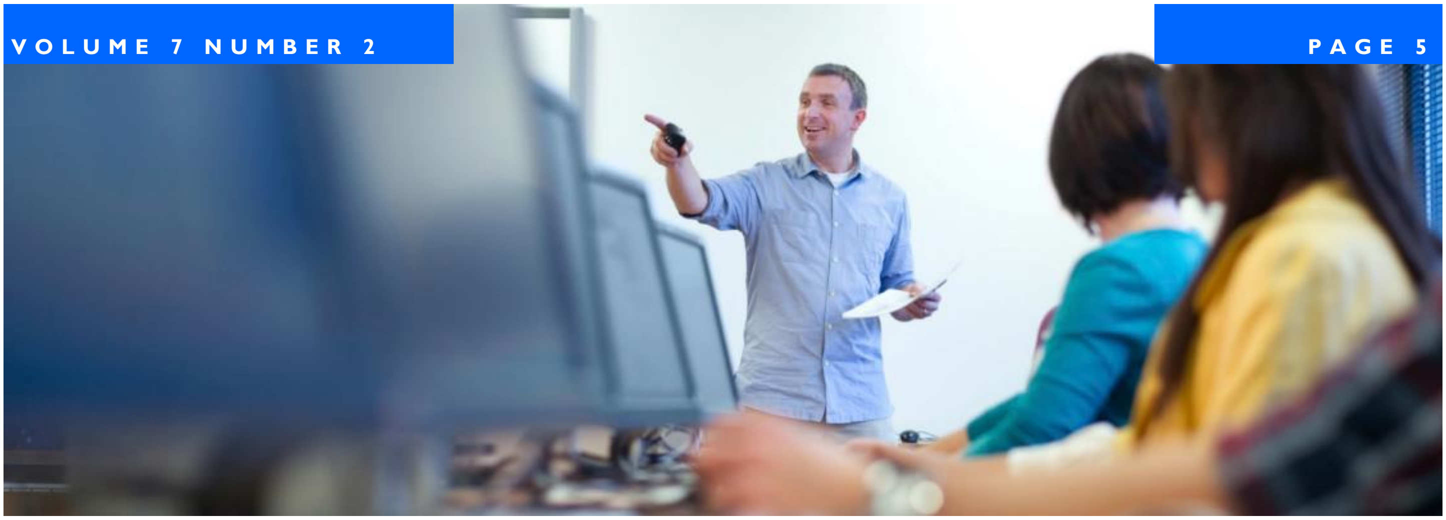
March 5, 2018

Interested?

For more information about this program, please contact:

Lauren Kirgis at Lauren.Kirgis@uc.edu

Submit your application online:
cech.uc.edu/it/cybersecurity/cybersecurity-camp



Mentorship Committee Update

Mentors and mentees will be invited to attend a group meeting in April. Location, date, and time details coming soon.

Mission Statement

Provide curious mentees at any stage of their information security career lifecycle with access to mentors who share their knowledge and experience in ensuring the confidentiality, integrity, and availability of information resources throughout a variety of industries.

Overview

The ISSA-COS Mentorship Program is designed to be mentee driven. Mentees determine the number of mentors they meet with depending on their questions, needs, and availability. The goal is to provide mentees with quality mentoring opportunities in a professional and problem solving environment. There will be group meetings twice a year (April & October) for all mentors and mentees to meet, greet, and discuss information security. Individual meetings between mentees and mentors will be scheduled throughout the year determined by the mentee and mentor. Mentees and mentors are expected to prepare for individual meetings by writing down questions and discussion topics prior to the meeting. e-Mentoring is also an option for those who need remote options. Mentors will meet as a group twice a year (January & June) to collaborate and share resources. Small group meetings to discuss specific topics and field trips to companies and organizations will be scheduled ad hoc.

Why Mentor?

Give back to the security community by sharing your knowledge and experience, provide career insight to mentees, grow your network.

Why be a Mentee?

Gain access to knowledge and experience in different security areas and industries.

Enrollment Process

- Be an ISSA Member
- Complete the Mentorship Enrollment Form
- Submit form with your resume to mentorship@issa-cos.org

ISSA Fellow Program

2018 Fellows Cycle Now Open

The Colorado Springs ISSA Chapter has over 500 current members. Many of you have been members for several years and may qualify for the ISSA fellow program. The Fellow Program recognizes sustained membership and contributions to the profession. If you think you or another ISSA associate may qualify in the fellow program, please contact Shawn P. Murray at 5871charlois@gmail.com or at 719-362-0666 to coordinate the process. Shawn is the chair of the chapter awards committee and will help you through the steps. Below are some additional details on the ISSA Fellow Program. Qualification information is also presented below:

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

Nominations and applications are accepted on an annual cycle. Applications will be accepted until March 23, 2018 at 5:00pm Eastern Time. Following the application period, there will be a ten week review period followed by the notification and presentation process. Fellows and Distinguished Fellows will be recognized at the 2018 ISSA International Conference.

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

To Become a Senior Member

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

Senior Member Qualifications

- 5 years of ISSA membership
- 10 years relevant professional experience

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

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

To Become a Fellow or Distinguished Fellow

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

Fellow Qualifications

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

(Continued on page 7)

Update Your Profile!

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

(Continued from page 6)

All Fellow applications require a nomination to qualify.

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

Distinguished Fellow Qualifications

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

All Distinguished Fellow applications require a nomination to qualify.

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

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

Shawn P. Murray

Awards & Recognition Committee Chair
5871charlois@gmail.com
719-362-0666

New NIST Forensic Tests Help Ensure High-Quality Copies of Digital Evidence

By NIST Staff, NIST, December 12, 2017

Data found on a suspect’s computer, cell phone or tablet can prove to be crucial evidence in a legal case. A new set of software tools developed at the National Institute of Standards and Technology (NIST) aims to make sure this digital evidence will hold up in court.

The software suite, referred to collectively as federated testing tools, is designed to help law enforcement and forensic practitioners with a critical early step in evidence collection: making a copy of the data from a seized electronic device. Because a suspect’s guilt or innocence can hang in the balance, both the prosecution and the defense must agree that the digital forensic process did not introduce any unseen errors into the data, and that the methods they are using work as expected.

Extracting and copying data is a risky process because of the rapidly shifting digital landscape that we and our devices inhabit. Confronting the practitioners are all the differences in data and format that can exist between one device and the next—because of the sheer number of different manufacturers, and because of the frequent software updates pushed to various makes and models.

“It’s hard to keep up,” said Barbara Guttman, one of the suite’s developers at NIST’s Computer Forensics Tool Testing project. “You don’t want to risk your copying software failing when you try to get data from some new computer that is critical to your case. So, we created these tools to help ensure that the copying software works effectively and transparently.”

NIST

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

The federated testing tools allow authorities to run tests in advance on their digital forensic software to make sure ahead of time that it will not fail them when a suspect’s personal computer, media or device arrives in the forensic science lab. Guttman describes the suite as the three most critical tools for evidence acquisition and preservation, each addressing one aspect of the copying process.

One tool tests software for copying computer disks, while another tests mobile device data extraction software. These two test protocols were available previously, but the suite is now completed with a new third test for “write blockers,” which are a sort of one-way valve for data-copying software. An effective write blocker allows data to flow only from the seized device to the copying computer, not the other way around. Later updates to the suite will address additional forensic functions, Guttman said.

The full suite is a freely available Linux file that anyone can download and burn to a blank CD. They can use the disk to boot their workstation and test their copying tools via a user-friendly interface.

The NIST software also allows different forensics labs to exchange the results of their tests with each other, so that they can share the burden of exploring how well a copying method works on a specific platform and operating system. Running copying software through its paces generates a report that disparate organizations can share among themselves or with the world, allowing them to indicate whether they found anomalies during the testing or not.

“Pooling these traceable results will mean less work for any given lab or organization,” Guttman said. “We don’t require they share the tests, but a rising tide should raise all boats.”

Guttman cautioned that the tools will not ensure that a copying or digital forensic process is flawless, only that the results of the job are clearly visible to anyone.

“Evidence doesn’t have to be complete to be admissible,” she said. “The key here is that copying does not introduce errors into the data that no one can see.”

Interest in federated testing will go beyond law enforcement agencies, Guttman added. Any organization that performs forensics, such as civil law firms and corporate enforcement offices, will find a use for the test suite.

Rights group criticises China for mass DNA collection in Xinjiang

By Reuters Staff , Reuters, December, 13 2017

Chinese authorities have collected DNA and other biometric data from the whole population of the volatile western region of Xinjiang, Human Right Watch said on Wednesday, denouncing the campaign as a gross violation of international norms.

Hundreds of people have been killed in Xinjiang in the past few years in violence between Uighurs, a mostly Muslim people, and ethnic majority Han Chinese, which Beijing blames on Islamist militants.

The unrest has fuelled a sweeping security crackdown there, including mass rallies by armed police, tough measures that rights advocates say restrict religious and cultural expression, and widespread surveillance.

Police are responsible for collecting pictures, fingerprints, iris scans and household registration information, while health authorities should collect DNA samples and blood type information as part of a “Physicals for All” programme, the New York-based group said in a statement, citing government a document.

“The mandatory databanking of a whole population’s biodata, including DNA, is a gross violation of international human rights norms, and it’s even more disturbing if it is done surreptitiously, under the guise of a free health care program,” Human Rights Watch’s China director Sophie Richardson said.

According to the Xinjiang-wide plan posted online by the Aksu city government in July, main goals for the campaign include collecting the biometric data for all people between the age of 12 and 65, and verifying the region’s population for a database.

“Blood type information should be sent to the county-level police bureaus, and DNA blood cards should be sent to the county police bureaus for inspection,” the plan said.

Data for “priority individuals” should be collected regardless of age, it said, using a term the government has adopted to refer to people deemed a security risk.

Government workers must “earnestly safeguard the peoples’ legal rights”, plan said, but it made no mention of a need to inform people fully about the campaign or of any option for people to decline to take part.

Xinjiang officials could not be reached for comment.

Chinese Foreign Ministry spokesman Lu Kang, asked about the report by Human Rights Watch, accused the group of making “untrue” statements.

He told a regular news briefing in Beijing the general situation in the region was good.

Human Rights Watch cited an unidentified Xinjiang resident saying he feared being labelled with “political disloyalty” if he did not participate, and that he had not received any results from the health checks.

State media, reporting on the campaign checks, have said participation was voluntary.

Read the rest here:

https://in.reuters.com/article/china-xinjiang/rights-group-criticises-china-for-mass-dna-collection-in-xinjiang-idINKBN1E71DU

(Continued from page 1)

ISSA International Awards

The 2018 ISSA International Awards Nomination period is also open, with nominations being accepted for several awards. Please let the Board know if you know someone who should be considered for one of these awards, or if you'd like to be considered for any of these awards. A brief description of each award is included below; further details can be found in the ISSA International Awards Policies and Procedures Manual, accessible via this webpage: https://www.issa.org/?page=Awards.

Hall of Fame Award: Induction into the ISSA Hall of Fame recognizes an individual's exceptional qualities of leadership of in their own careers and organizations as well as an exemplary commitment to the information security profession. Honorees must represent the highest levels of professionalism and lifetime achievement. In order to achieve this level a candidate must be in the information systems security field for a minimum of 10 years.

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

Security Professional of the Year Award: The Security Professional of the Year Award honors one (1) individual who best exemplifies the most outstanding standards and achievement in information security in the preceding year.

Volunteers of the Year: These Volunteers of the Year Awards recognize no more than five (5) members who have made a significant difference to any of their chapter, the association, or the information security community through dedicated and selfless service to ISSA.

Outstanding Organization of the Year Award: Candidate organizations must have provided a sustained, proactive presence that directly contributed to the overall good and professionalism of the Association and its membership, providing either services, products, and or direct support that ensures the promotion of the highest ethical standards in addressing Information Security and its future direction.

Chapter of the Year Awards: Chapter of the Year recognizes chapters that have done an exceptional job of supporting ISSA's mission, serving their member communities and provide enabling opportunities. Awards will be made in up to three categories based on size: Fewer than 100 Members (Small Chapter), 101-300 members (Medium Chapter), and More than 300 members (Large Chapter).

President's Award for Public Service: This award is for recognition of an individual's contribution to the information security profession in the area of public service. ISSA membership is not required for this award. Honorees must have a tangible presence and recognition by the general public, either by name, or by the research that they have presented to the general public through the organization or media that they represent.

Let's recognize our exceptional members! Contact any Board member, or the Recognition Committee, if you have any questions.

Colleen

ISSA

Chapter of the Year 2017

How an Ohio Hospital Avoided a Widespread Ransomware Attack

By Elizabeth Snell, Health IT Security, December 04, 2017

Having the necessary and applicable data security tools in place, along with comprehensive employee education, are critical for ransomware attack prevention measures. Organizations of all sizes need to be aware of the potential threats and be willing to invest in options that will help keep sensitive data secure.

Ohio-based Wood County Hospital averted a potentially widespread ransomware attack by detecting the issue with the help of its managed security services provider (MSSP) two weeks before it surfaced.

CIO Joanne White said the organization had been wanting to increase its security by adding network traffic analytics.

Wood County Hospital has 19 clinics it supports, White explained to *HealthITSecurity.com.* There are 16 people in IT who supports all of those locations. Wood County utilizes Cerner for its hospital EMR and NextGen in the clinics, she added.

The ransomware incident took place in September 2016, which is when an employee received a popup message that said files had been encrypted and that Wood County had 72 hours to pay.

“We had been doing a proof of concept with ExtraHop,” White recalled, adding that preconfigured reports and dashboards were already prebuilt with ExtraHop. “We had done a proof of concept, collecting data, and we were looking at things for the new fiscal year. It was still collecting data in the background, but we hadn't looked at it since ExtraHop had done a call with us to review the details of our testing period.”

White added that Wood County immediately contacted ExtraHop after the ransomware was first discovered, asking if Wood County could access the reports in the system to determine what was happening.

“The first thing we saw was one PC that was sending pings all over our entire network,” White said. “It was just flooding our internal network, so we focused on that machine. The first thing we did was we pulled it off the network. Then we brought it over into IT and we looked through the others.”

Wood County dug into the ExtraHop logs to see the anomalies, she continued. The organization also uses Veriato 360 to view keystrokes.

“From the logs that we were able to locate through ExtraHop, we saw the timestamp on the ransomware file,” White explained. “We looked at [Veriato 360] for that timeframe and we were able to pinpoint exactly where the ransomware came in the system.”

“It was a nurse in behavioral health who had clicked on a website that she goes to on a frequent basis for her job,” she continued. “It was at the minute she clicked on a link in their website that the ransomware entered our system.”

Wood County was able to isolate the device from the main network, along with terminal services that the computer had connected to. White added that Wood County ran scans and continued to work with ExtraHop to ensure that the ransomware did not spread.

“We found 47 instances of the infected directory that could not propagate due to no admin rights,” White stated. “We had 47 executables waiting to take off. Can you imagine how we were feeling at that point, knowing what a disaster it could have been?”

“At that point we reimaged the PC,” White added. “We reimaged the server. We deleted [the employee’s] user profile, and of course deleted her user directory. We created new ones and we set up scans and alerts in ExtraHop.”

The ransomware was a new strain called CryptFile2. The message stated that decrypting the Wood County files was only possible with the necessary private key and decrypt program, which was on a “Secret Server.”

Read the rest here:

https://healthitsecurity.com/news/how-an-ohio-hospital-avoided-a-widespread-ransomware-attack

How Antivirus Software Can Be Turned Into a Tool for Spying

By Nichole Perlroth, New York Times, January 1, 2018

It has been a secret, long known to intelligence agencies but rarely to consumers, that security software can be a powerful spy tool.

Security software runs closest to the bare metal of a computer, with privileged access to nearly every program, application, web browser, email and file. There's good reason for this: Security products are intended to evaluate everything that touches your machine in search of anything malicious, or even vaguely suspicious.

By downloading security software, consumers also run the risk that an untrustworthy antivirus maker — or hacker or spy with a foothold in its systems — could abuse that deep access to track customers' every digital movement.

"In the battle against malicious code, antivirus products are a staple," said Patrick Wardle, chief research officer at Digita Security, a security company. "Ironically, though, these products share many characteristics with the advanced cyberespionage collection implants they seek to detect."

Mr. Wardle would know. A former hacker at the National Security Agency, Mr. Wardle recently succeeded in subverting antivirus software sold by Kaspersky Lab, turning it into a powerful search tool for classified documents.

Mr. Wardle's curiosity was piqued by recent news that Russian spies had used Kaspersky antivirus products to siphon classified documents off the home computer of an N.S.A. developer, and may have played a critical role in broader Russian intelligence gathering.

"I wanted to know if this was a feasible attack mechanism," Mr. Wardle said. "I didn't want to get into the complex accusations. But from a technical point of view, if an antivirus maker wanted to, was coerced to, or was hacked or somehow subverted, could it create a signature to flag classified documents?"

That question has taken on renewed importance over the last three months in the wake of United States officials' accusations that Kaspersky's antivirus software was used for Russian intelligence gathering, an accusation that Kaspersky has rigorously denied.

Last month, Kaspersky Lab sued the Trump administration after a Department of Homeland Security directive banning its software from federal computer networks. Kaspersky claimed in an open letter that "D.H.S. has harmed Kaspersky Lab's reputation and its commercial operations without any evidence of wrongdoing by the company."

For years, intelligence agencies suspected that Kaspersky Lab's security products provided a back door for Russian intelligence. A draft of a top-secret report leaked by Edward J. Snowden, the former National Security Agency contractor, described a top-secret, N.S.A. effort in 2008 that concluded that Kaspersky's software collected sensitive information off customers' machines.

The documents showed Kaspersky was not the N.S.A.'s only target. Future targets included nearly two dozen other foreign antivirus makers, including Checkpoint in Israel and Avast in the Czech Republic.

At the N.S.A., analysts were barred from using Kaspersky antivirus software because of the risk it would give the Kremlin broad access to their machines and data. But excluding N.S.A. headquarters at Fort Meade, Kaspersky still managed to secure contracts with nearly two dozen American government agencies over the last few years.

Last September, the Department of Homeland Security ordered all federal agencies to cease using Kaspersky products because of the threat that Kaspersky's products could "provide access to files."

A month later, The New York Times reported that the Homeland Security directive was based, in large part, on intelligence shared by Israeli intelligence officials who successfully hacked Kaspersky Lab in 2014. They looked on for months as Russian government hackers scanned computers belonging to Kaspersky customers around the world for top secret American government classified programs.

In at least one case, United States officials claimed Russian intelligence officials were successful in using Kaspersky's software to pull classified documents off a home computer belonging to Nghia H. Pho, an N.S.A. developer who had installed Kaspersky's antivirus software on his home computer. Mr. Pho pleaded guilty last year to bringing home classified documents and writings, and has said he brought the files home only in an attempt to expand his résumé.

Read the rest here:

https://www.nytimes.com/2018/01/01/technology/kaspersky-lab-antivirus.html?emc=edit_th_20180102&nl=todaysheadlines&nlid=1043739&_r=0

Blackout: Critical Infrastructure Attacks Will Soar in 2018

By Adam Levin, Inc, Undated

There was a stunning cyberattack on a critical Middle Eastern infrastructure site recently and it hasn't gotten the public scrutiny it deserves. Triton (A.K.A. Trisis), a new strain of malware, was discovered last month via intelligence sharing reports provided by the security vendors FireEye and Dragos. The news was the latest in a series of public disclosures about progressively more sophisticated energy plant hacks.

The specter of attacks on the power grid and other systems is no longer a matter of speculation. Hackers are testing the protections for critical infrastructure, and energy plant operators need to take the threat seriously, as do the decision makers in the industrial sector at large.

Core finding

Security analysts uncovered malware designed to take over the Schneider Electric Triconex Safety Instrumented System (SIS) at an unnamed industrial site. SIS systems are routinely used in plant settings to monitor industrial processes, and shut them down if operating parameters approach a dangerous state.

Notably, it now appears that the Triton hackers inadvertently shut off the plant's SIS system in what may have been a botched reconnaissance operation, says Phil Neray, strategy vice president at Boston-based cybersecurity vendor CyberX.

"They had hacked into the controller of the safety system, which is there to shut everything down if something goes wrong," Neray observes. "They evidently made a mistake and triggered the safety system to shut down the plant."

Hacking methodology

Experts say it's likely that the hackers initially used social engineering, perhaps a phishing ruse that prompted a plant employee to unwittingly share logon credentials to the SIS. The hackers would then have been able to embed the Triton malware in the SIS, and gain access to the system.

"Reconnaissance, pivoting, and dwelling at length within networks are common strategies for advanced hackers," says Satya Gupta, chief technology officer at Virsec Systems, a supplier of application security systems. "Their goal certainly would have been bigger than to trip a relatively benign shutdown."

This is a type of activity one would expect from rival nations preparing offensive and defensive strategies for cyberwar campaigns. As the attack vector becomes more defined, it gives rise to a question: How long have hackers been targeting infrastructure, and which past attacks were part of that campaign? That is unknowable, but the Triton revelation could change the way researchers view the Shamoon virus outbreaks that crippled office computers at Saudi energy companies in December 2012, and again in January 2017.

Wider implications

While stealth and misdirection are ruling principles in cyberwarfare--making attribution difficult if not impossible, it seems worth noting the Triton disclosure closed out a year in which hacking groups believed to be aligned with Russia, Iran and North Korea have been caught probing and accessing the back-office business networks of U.S. energy companies.

This flurry of activity prompted the FBI and the Department of Homeland Security to issue an amber alert warning about a wave of malware attacks targeting office workers at U.S. energy plants. Why go after office workers? Humans are always the weakest link in any security system. Industrial control systems are disconnected, or "air-gapped," from administrative systems, and thus considered intrinsically safe--but the people who operate them are not.

Malicious hackers are very good at what they do. Increased use of cloud computing and connected mobile devices (with questionable security) has made air-gapped security obsolete, and given rise to an incipient security nightmare. The alarming accomplishment of the Triton caper was the demonstration of how a phishing attack on the IT side of the house can be leveraged to hack into the OT, or operational technology, side of the house.

Read the rest here:

https://www.inc.com/adam-levin/next-hackers-target-industrial-plants-critical-infrastructure.html

Windows 10 can now show you all the data it's sending back to Microsoft

By Frederic Lardinois, TechCrunch, January 24, 2018

A recent technical alert is issued based on information from Department of Homeland Security and the Federal Bureau of Investigation about ongoing cyberattacks against critical industrial infrastructure and control systems across the United States.

Microsoft's and its partners' engineers use the telemetry data from Windows 10 to diagnose crashes, learn about its users hardware configurations and more. It's on by default and while Microsoft tells you that it collects this data and gives you a choice between basic (the default setting) and "full" diagnostics, it never allowed you to actually see exactly what was being sent back to Redmond. That's changing now, though. Windows 10 insiders will soon be able to install a new program from the Microsoft Store, the "Windows Diagnostic Data Viewer," that gives them full access to all the diagnostic data from their Windows device.

As Marisa Rogers, Microsoft's privacy officer for its Windows and Devices Group, told me, the idea here is to give users the option to see "that next layer of transparency from Microsoft" and allow them to verify that the company is doing what its documentation says. Users can download this free tool without the need for a Microsoft account.

Microsoft itself, of course, has long had tools to view this data internally, but the Data Viewer tool puts a user-friendly interface on top of this data.

What kind of data can you expect to see? Here is Microsoft's list:

- Common Data, like the Operating System’s name, the Version, Device ID, Device Class,Diagnostic level selection and so on.
- Device Connectivity and Configuration such as device properties and capabilities, preferences and settings, peripherals, and device network information.
- Product and Service Performance data that show device health, performance and reliability data, movie consumption functionality on the device and device file queries. It’s important to note that this functionality is not intended to capture user viewing or, listening habits.
- Product and Service Usage data includes details about the usage of the device, operating system, applications and services.
- Software Setup and Inventory such as installed applications and install history, device update information.

While Microsoft hopes that this tool allows users to validate and verify what it has been telling them all along, it may still come as a shock to some people that Microsoft is collecting this data by default, even if it's only technical data about their devices. "I hope that people have been paying attention to the messaging we have been providing over the last few month," Rogers said. But outside of the world of Microsoft enthusiasts, few people are probably even fully aware of this telemetry program, so it'll be interesting to watch the reaction.

Read the rest here:

https://techcrunch.com/2018/01/24/windows-10-can-now-

Top 8 Cybersecurity Skills IT Pros Need in 2018

By Dawn Kawamoto, Dark Reading, December 18, 2017

One-fifth of CIOs expect to expand their IT teams in the first half of 2018, a new report found, and nearly one quarter of the respondents cite cybersecurity as their top priority.

The survey results in the the Robert Half Technology IT Hiring Forecast and Local Trends Report also found that 43% of respondents point to cybersecurity as the technical skill in highest demand at their organization.

"When we entered 2017, the talking points were about bridging the gap between security and IT. But with sophisticated technical breaches and ransomware attacks like WannaCry, there is a return back to incident response and more technical skills, which are hard to find," says Owanate Bestman, information security contract consultant at Barclay Simpson..

As for technical skills, "play to your strengths," Bestman advises. "If you are a generalist IT manager, a business-facing security manager role that buys security software for the organization or launches security training may work. Or, if you are a network architect, then potentially you could make the transition to a security network architect."

Read the rest here:

https://www.darkreading.com/careers-and-people/top-8-cybersecurity-skills-it-pros-need-in-2018/d/d-id/1330657

FBI Software For Analyzing Fingerprints Contains Russian-Made Code, Whistleblowers Say

By Chris Hamby, BuzzFeed News, Undated

The fingerprint-analysis software used by the FBI and more than 18,000 other US law enforcement agencies contains code created by a Russian firm with close ties to the Kremlin, according to documents and two whistleblowers. The allegations raise concerns that Russian hackers could gain backdoor access to sensitive biometric information on millions of Americans, or even compromise wider national security and law enforcement computer systems.

The Russian code was inserted into the fingerprint-analysis software by a French company, said the two whistleblowers, who are former employees of that company. The firm — then a subsidiary of the massive Paris-based conglomerate Safran — deliberately concealed from the FBI the fact that it had purchased the Russian code in a secret deal, they said.

In recent years, Russian hackers have gained access to everything from the Democratic National Committee's email servers to the systems of nuclear power companies to the unclassified computers of the Joint Chiefs of Staff, according to US authorities.

This September, the Department of Homeland Security ordered all federal agencies to stop using products made by the Moscow-based company Kaspersky Lab, including its popular antivirus software, and media outlets reportedthat Russian hackers had exploited it to steal sensitive information on US intelligence programs. The department later clarified that the order didn't apply to "Kaspersky code embedded in the products of other companies." The company's founder, Eugene V. Kaspersky, has denied any involvement in or knowledge of the hack.

The Russian company whose code ended up in the FBI's fingerprint-analysis software has Kremlin connections that should raise similar national security concerns, said the whistleblowers, both French nationals who worked in Russia. The Russian company, Papillon AO, boasts in its own publications about its close cooperation with various Russian ministries as well as the Federal Security Service — the intelligence agency known as the FSB that is a successor of the Soviet-era KGB and has been implicated in other hacks of US targets.

Cybersecurity experts said the danger of using the Russian-made code couldn't be assessed without examining the code itself. But "the fact that there were connections to the FSB would make me nervous to use this software," said Tim Evans, who worked as director of operational policy for the National Security Agency's elite cyberintelligence unit known as Tailored Access Operations and now helps run the cybersecurity firm Adlumin.

The FBI's overhaul of its fingerprint-recognition technology, unveiled in 2011, was part of a larger initiative known as Next Generation Identification to expand the bureau's use of biometrics, including face- and iris-recognition technology. The TSA also relies on the FBI fingerprint database.

In hopes of winning the FBI contract, the Safran subsidiary Sagem Sécurité, later renamedMorpho, licensed the Papillon technology to boost the performance of its own fingerprint-recognition software, the whistleblowers said. Both of them worked for Morpho: Philippe Desbois was the former CEO of the company's operations in Russia, and Georges Hala worked for Morpho's business development team in Russia.

BuzzFeed News reviewed an unsigned copy of the licensing agreement between the French and Russian companies, which both men said they had obtained while working for Morpho; it is dated July 2, 2008 — a year before the company beat out some of the world's largest biometric firms, including an American competitor, to secure the FBI business. It grants Sagem Sécurité the right to incorporate the Papillon code into the French company's software and to sell the finished product as its own technology. It also stipulates that Papillon would provide updates and improvements during the five-year period that ended on the last day of 2013. In return, Sagem Sécurité agreed to pay an initial fee of roughly 3.8 million euros — equivalent to almost $6 million at the time — plus annual fees.

The contract, which is also referenced in court documents, says that to Papillon's knowledge its software does not contain any "undisclosed 'back door,' 'time bomb,' 'drop dead,' or other software routine designed to disable the software automatically with the passage of time or under the positive control of any person" or any "virus, 'Trojan horse,' 'worm,' or other software routines or hardware components designed to permit unauthorized access, to disable, erase, or otherwise harm the software, hardware, or data."

Read the rest here:

https://www.buzzfeed.com/chrishamby/fbi-software-contains-russian-made-code-that-could-open-a?utm_term=.lb9ZGvdLN#.ouOM9RdBe

British teenager hacked top ranking US officials using social engineering

By Zeljka Zorz, HelpNetSecurity, January, 22, 2018

How did British teenager Kane Gamble, who at the time was only 15 years old, manage to break into email accounts of the CIA and DNI chiefs, as well as gain access to a number of sensitive databases and plans for intelligence operations in Afghanistan and Iran?

The answer is social engineering.

A day in court

Gamble, who was part of Crackas With Attitude (CWA), a group of hackers with a pro-Palestinian agenda, pleaded guilty to ten offenses under the computer misuse act at Leicester crown court in October 2017.

Last week, in preparation for sentencing, Crown Court judge Sir Charles Anthony Haddon-Cave has been informed of the details of his exploits, which took place between June 2015 to February 2016.

According to the information provided by the prosecutors, Gamble managed to gain access to the Verizon internet account and private AOL email account of then-CIA Director John Brennan, and extract sensitive information from it.

He did so via phone, by pretending to be a Verizon employee in order to trick the company into sharing personal information about Brennan, then using that information to impersonate Brennan to get AOL to reset the password associated with the email account. Ultimately, he managed to trick the help desk handlers into changing the security questions and security number. According to The Telegraph, Gamble eventually gained access to Brennan's emails, contacts, his iCloud storage account and his wife's iPad.

By employing the same tactics, he also managed to compromise the Verizon broadband account and personal email account of James Clapper, the US Director of National Intelligence at the time. In addition to this, he impersonated Clapper on the phone and succeeded in making Verizon set up call-forwarding to divert calls made to Clapper's home phone to the Free Palestine movement.

Gamble's other victims included:

- Jeh Johnson, the then-Secretary of Homeland Security. Again, Gamble used a similar approach to gain access to Johnson's phone, and used that access to listen to his voicemails and send texts from his phone.
- Mark Giuliano, FBI's Deputy Director at the time. Gamble gained access to his home accounts by pretending to be him and then used the information to repeatedly gain to access the FBI's Law Enforcement Enterprise Portal, even after the password was changed. Gamble used this access to steal and post online personal details of Officer Darren Wilson (who shot and killed black teenager Michael Brown in Ferguson, Missouri).
- John Holdren, the senior science and technology adviser to former US president Barack Obama. With the help of an accomplice, Gamble also managed to get Holdren's house "swatted."
- Avril Haines, the White House deputy national security adviser at the time, and FBI Special Agent Amy Hess – he accessed their private calls and emails, and gained access to Hess's computer.
- The US Department of Justice. Gamble gained access to details about FBI employees and case files, and later published some of that sensitive information online.

As the prosecutors pointed out, CWA has incorrectly been referred to as hackers, as they mostly used social engineering to trick call centers or help desks into helping them get access to email accounts, phones, computers and law enforcement portals.

Read the rest here:

https://www.helpnetsecurity.com/2018/01/22/hack-social-engineering/

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.

CISSP Study Guide Discount

Ashley Edwards, Senior Account Manager, Wiley

aedwards@wiley.com

CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide: Edition 7

50% off for ISSA chapters

Promo code **CSP50**

Items of Interest

GET A JOB!

Colorado Springs ISSA chapter member Melody Wilson maintains a "Jobs" page at *Cyberjoblist.com*. There is no charge. The jobs are set to remain listed for 30 days. Job listing originators re-post them again for another 30 days. It is designed for Colorado Springs, but once in awhile a job is listed outside the area.

You can also sign-up on the *Cyberjoblist.com* site for Job Alerts to be notified when a new job listing is posted!

ISSA Photos are courtesy of our Chapter Photographer

Warren Pearce.

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

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: Erik Hjelmstad

Communications Officer: Anna Johnston
- Dep. Communications Officer: **Vacant**

Recorder/Historian: Erik Huffman
- Deputy Recorder/Historian: **Vacant**

Member at Large: James Asimah
Member at Large: Dawn Wellein
Member at Large: Ryan Schneider
Member at Large: Jim Blake
Dir. of Certification: Derek Isaacs
- Dep Dir Certifications: Kurt Danis

Dir. of Professional Outreach: **Vacant**
- Dep Dir. of Professional Outreach: June Shores

Committee Chairs:

Ethics: Tim Westland
Web Development: Bill Welker
Sponsorship: Dr. Pat Laverty
Mentorship: Melissa Absher
Recognition: Shawn P. Murray
Sponsorship: Pat Laverty
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:

doncreamer@outlook.com

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

Smartphone Battery Explodes After Man Inexplicably Bites Into It

By David Moye, Huffpost, January 23, 2018

Chew on this: A man in China decides he needs to verify if a smartphone battery is legit — so he bites it?!?!?

It’s a decision that literally blew up in his face, as the now-viral video above demonstrates.

Security camera footage captured Jan. 19 at a store in Nanjing City, Jiangsu Province, shows the unidentified man biting into the iPhone battery, presumably to check its authenticity.

Read the rest here:

https://finance.yahoo.com/news/smartphone-battery-explodes-man-inexplicably-200335454.html

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