ISSA Information Systems Security Association Colorado Springs Chapter

WWW.ISSA-COS.ORG

Colorado Springs, Colorado

ISSA-COS NEWSLETTER

VOLUME 8 NUMBER 11 NOEMBER 2019

Welcome to November!

A Note From Our President

By Mr. Ernest Campos

Fellow Members of ISSA-COS,

Can you believe we already had **three** snowstorms before November even began!? Ahh… life in Colorado Springs.

Fortunately, the early winter weather did not slow down our chapter. We gathered incredible momentum during the 3rd quarter of the year and we are maintaining the pace as we pull into the 4th quarter. So much so, our planning efforts are ahead of schedule, and I believe we will all be able to slow down in December and enjoy the holidays.

Before we enjoy a sneak peek into the future, lets take a moment to review what we did last month. Looking back at October, our chapter participated in **National Cybersecurity Awareness Month**. Our contributions to the month included hosting a panel discussion for both our dinner and lunch events. The topic of the discussion was "**Cybersecurity in COS: Past, Present, and Future**." For the dinner event, our moderator was **Ms. Gretchen Bliss** (Pikes Peak Community College) and for the lunch event, our moderator was **Mr. Vinnie Persichetti** (COS Chamber and EDC). Our panel members for both events included: **Dr. Rick White** (University of Colorado, Colorado Springs), **Mr. Mike Schmidt** (National Cyber Exchange), **Mr. Russ White** ((ISC)^2), **Dr. Bob Cook** (University of Colorado, Colorado Springs), **Ms. Erin Miller** (National Cybersecurity Center), and **Mr. Mark Spencer** (ISSA-COS Past President Emeritus). These panel discussions provided our members with a glimpse of the past, learning how our region become such a prominent hub for the Cybersecurity industry. It also provided awareness of all the various organizations that participate in our local Cybersecurity ecosystem and the ways in which they contribute. As for our monthly Mini Seminar, we enjoyed an encore presentation from **Ms. Erin Miller** (National Cybersecurity Center) as she educated us on the selection of NCC to host the newly commissioned **Space ISAC (Information Sharing and Analysis Center)**, what that means for our community, and the significate mission the Space ISAC will play for our nation. We also heard **from Mr. Frank Gearhart** (ISSA-COS Past President) as he shared "***Blockchain: Current Use, Future Use, and What It Means for Us.***" As if all those events weren't enough, our chapter was also invited to

(Continued on page 4)

Researchers Say They Uncovered Uzbekistan Hacking Operations Due to Spectacularly Bad OPSEC

By Kim Zetter, Motherboard, October 3, 2019

Nation-state spy agencies are only as good as their operational security—the care they take to keep their digital spy operations from being discovered. But occasionally a government threat actor appears on the scene that gets it all wrong.

This is the case with a threat actor recently discovered by Kaspersky Lab that it's calling SandCat—believed to be Uzbekistan's repressive and much-feared intelligence agency, the State Security Service (SSS).

The group's lax operational security includes using the name of a military group with ties to the SSS to register a domain used in its attack infrastructure; installing Kaspersky's antivirus software on machines it uses to write new malware, allowing Kaspersky to detect and grab malicious code still in development before it's deployed; and embedding a screenshot of one of its developer's machines in a test file, exposing a major attack platform as it was in development. The group's mistakes led Kaspersky to discover four zero-day exploits SandCat had purchased from third-party brokers to target victim machines, effectively rendering those exploits ineffective. And the mistakes not only allowed Kaspersky to track the Uzbek spy agency's activity but also the activity of other nation-state groups in Saudi Arabia and the United Arab Emirates who were using some of the same exploits SandCat was using.

"I'd call [SandCat] my zero-day Pez dispenser," Bartholomew told Motherboard, "because it seemed like every time we'd [find] another zero-day and patch it, they'd come up with another one. "

"These guys [Uzbekistan's intelligence agency] have been around for quite a long time and up until now I'd never heard of Uzbekistan having a cyber capability," said Brian Bartholomew, a researcher with Kaspersky's Global Research and Analysis Team who will present his findings about SandCat today in London at the VirusBulletin conference. "So it was kind of a shocker to me to know that they ... were buying all of [these exploits] and targeting all these people and yet no one has ever written about them."

The SSS, previously known as the National Security Service, isn't new to the spy game: It emerged in 1991 with the collapse of the Soviet Union to succeed the KGB as Uzbekistan's national intelligence agency and secret police, adopting some of the KGB's surveillance technologies as well as its oppressive tactics. Known for its torture and human rights abuses, the SSS was revamped in early 2018 by the country's new president, who sought to reform its repressive ways. But earlier this year the new head of the spy agency was booted after a year on the job, reportedly amid allegations that the agency had turned its spying capabilities against the new president and his family.

The agency's interest in offensive hacking operations were first exposed in 2015 when a hacker named Phineas Fisher hacked the Hacking Team, an Italian firm that sells hacking tools to governments and law enforcement agencies, and published thousands of emails exposing the company's correspondence with customers, including the SSS. According to the emails, which cover the years 2011-2015, the SSS spent nearly a million dollars on Hacking Team tools. But its hacking operations have gone largely unnoticed until recently.

In October 2018, researchers at Kaspersky stumbled across SandCat after discovering an already known piece of malware called Chainshot on a victim's machine in the Middle East. Chainshot had been used by two other nation-state threat actors in the Middle East in the past—groups security researchers have attributed to the UAE and Saudi Arabia—but the malware in this case was using infrastructure not associated with either of these countries, suggesting it was a different group Kaspersky hadn't seen before. SandCat was also using a zero-day exploit to install Chainshot.

As Kaspersky analyzed machines infected with the exploit and Chainshot, and began to dig into the group's infrastructure that was tied to the infections, it ultimately led Kaspersky to discover three more zero days used by the same group each of which got essentially burned as the vulnerabilities they attacked got patched

Read the rest here:

https://www.vice.com/en_us/article/3kx5y3/uzbekistan-hacking-operations-uncovered-due-to-spectacularly-bad-opsec

Membership Corner

Membership Update

First, I would 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.

New Members October
Samuel Chamberlin
Deana Patrick
John Kolodgy
Keith Golden
Cyrus Field Jr

Our membership is at ~431 members as of the end of October. Please watch the Newsletter, communications and eVites to ensure you stay aware of what's going on in the chapter. As always, if you have any membership questions don't hesitate to contact me.

Thanks,

David Reed

Membership Committee Chairman

membership@issa-cos.org

A Quick Guide to Sniffing Attacks

By Ryan Stewart, Cyware, October 6, 2019

Sniffing is commonly performed by system administrators to troubleshoot or analyze the network. Hackers abuse this technique to perform cyber attacks.

How does it work?

The Network Interface Cards (NICs) by default ignore any traffic that is not addressed to them.

- Sniffing attacks involve turning the NICs to promiscuous mode. This enables the NICs to receive all the traffic on the network.
- By decoding the encapsulated information in the data packets, sniffers can listen to all the traffic through the NICs.
- Weakly encrypted data packets make sniffing attacks easier to perform.

Types of sniffing

There are two types of sniffing - active and passive.

- Active sniffing involves injecting address resolution protocols (ARPs) into a network to flood the switch content address memory (CAM) table. This, in turn, will redirect legitimate traffic to other ports, allowing the attacker to sniff traffic from the switch.
- Active sniffing techniques include spoofing attacks, DHCP attacks, and DNS poisoning among others.
- Passive sniffing involves only listening and is usually implemented in networks connected by hubs. In this type of network, the traffic is visible to all hosts.

Read the rest here:

https://cyware.com/news/a-quick-guide-to-sniffing-attacks-44edd76b

(Continued from page 1)

attend the **Cybersecurity Summit for Small Businesses**, hosted by the COS Small Business Development Center (SBDC). At this event, we hosted a booth for our chapter and provided guest speakers throughout the day. **THANK YOU**, guest speakers and community partners, for contributing to the professional development of our region and to our chapter!

A Note From Our President

Returning our focus back on November, this month represents our final opportunity to attend chapter meetings and a Mini Seminar in 2019. This month, to avoid conflicting with early Thanksgiving travel plans, **we have moved our Mini Seminar to Saturday, 11/16**. Our dinner and lunch meetings will still take place during the 3rd full week of the month; 11/19 and 11/20, respectively. Also, during November, we will complete our Annual Election process to help solidify our 2020 Board of Directors. Make sure you participate to help exercise your rights. Finally, be sure you **SAVE THE DATE**, our **Annual Award Ceremony** will take place on Thursday, 12/5 from 11:00 – 1:00 PM. This is a lunch event that will be held at the SCP Hotel. Registration will soon open for this event.

Now, about that 2020 sneak peek I mentioned earlier. Next year will be a great year for our chapter. Many significant events will occur next year. Here is a list to just a few…

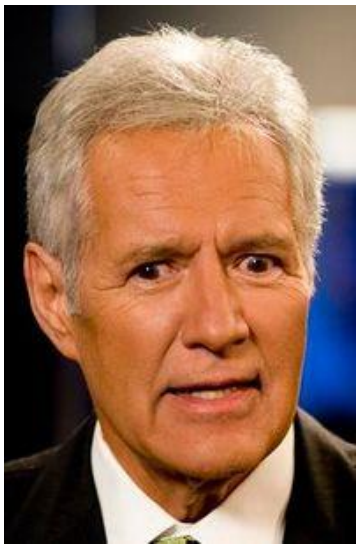
- The **10th Anniversary** of Peak Cyber symposium
- The institution of **Strategic Partnerships** designed to provide added value to our General Members
- An opportunity to become a "Big Brother" chapter to the soon-to-hatch **ISSA Pueblo Chapter**
- The introduction of a **new quarterly events** that will provide a much-needed service to our community that no other non-profit organization in our city is currently providing
- The institution of **new policies** that will enable our chapter to better utilize our funds, reduce waste, and afford to increase the quality of regularly scheduled events.

More details will follow in the December newsletter leading up to a full rollout of updates at the **January 2020 Annual President's Address and General Chapter Meeting**.

In closing, our Board of Directs hopes you will take advantage of our final programing for 2019. We appreciate all you have done for our chapter, for your employers, and for our community. We will have much to celebrate when we look back at 2019 and much to look forward to as we prepare for 2020.

Sincerely,

Ernest



Cybersecurity Jeopardy

Types of encryption

1. Uses two keys to encrypt plain text
2. Uses only one secret key that is possessed by both parties
3. RSA, Diffie-Hellman, and El Gamal are examples of this type of encryption
4. AES, DES, and 3DES are examples of this type of encryption

Identity and Access Management

1. Fences, security guards, and motion detectors are examples of this type of control
2. Palm topology and retina patterns are examples of this type of authentication factor
3. A ticket-based authentication protocol that helps protect against replay attacks
4. This protocol centralizes authentication for remote connections

The answers may be found in this newsletter.

U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack -officials

By Idrees Ali and Phil Stewart, Reuters, October 16, 2019

A new report by University of Minnesota researchers indicates cyberattacks pose a rising threat to food production and safety.

The United States carried out a secret cyber operation against Iran in the wake of the Sept. 14 attacks on Saudi Arabia's oil facilities, which Washington and Riyadh blame on Tehran, two U.S. officials have told Reuters.

The officials, who spoke on condition of anonymity, said the operation took place in late September and took aim at Tehran's ability to spread "propaganda."

One of the officials said the strike affected physical hardware, but did not provide further details.

The attack highlights how President Donald Trump's administration has been trying to counter what it sees as Iranian aggression without spiraling into a broader conflict.

Asked about Reuters reporting on Wednesday, Iran's Minister of Communications and Information Technology Mohammad Javad Azari-Jahromi said: "They must have dreamt it," Fars news agency reported.

The U.S. strike appears more limited than other such operations against Iran this year after the downing of an American drone in June and an alleged attack by Iran's Revolutionary Guards on oil tankers in the Gulf in May.

The United States, Saudi Arabia, Britain, France and Germany have publicly blamed the Sept. 14 attack on Iran, which denied involvement in the strike. The Iran-aligned Houthi militant group in Yemen claimed responsibility.

Publicly, the Pentagon has responded by sending thousands of additional troops and equipment to bolster Saudi defences - the latest U.S. deployment to the region this year.

The Pentagon declined to comment about the cyber strike.

"As a matter of policy and for operational security, we do not discuss cyberspace operations, intelligence, or planning," said Pentagon spokeswoman Elissa Smith.

GULF TENSIONS RISE SHARPLY

The impact of the attack, if any, could take months to determine, but cyber strikes are seen as a less-provocative option below the threshold of war.

"You can do damage without killing people or blowing things up; it adds an option to the toolkit that we didn't have before and our willingness to use it is important," said James Lewis, a cyber expert with the Washington-based Center for Strategic and International Studies.

Lewis added that it may not be possible to deter Iranian behavior with even conventional military strikes.

Tensions in the Gulf have escalated sharply since May 2018, when Trump withdrew from the 2015 Joint Comprehensive Plan of Action with Tehran that put limits on its nuclear program in exchange for the easing of sanctions.

It was unclear whether there have been other U.S. cyber attacks since the one in late September.

Iran has used such tactics against the United States. This month, a hacking group that appears linked to the Iranian government tried to infiltrate email accounts related Trump's re-election campaign.

Over 30 days in August and September, the group, which Microsoft dubbed "Phosphorous," made more than 2,700 attempts to identify consumer accounts, then attacked 241 of them.

Tehran is also thought to be a major player in spreading disinformation.

Read the rest here:

https://news.yahoo.com/exclusive-u-carried-secret-cyber-105108522.html

The DNA database used to find the Golden State Killer is a national security leak waiting to happen

By Antonio Regalado, MIT Technology Review, October 30, 2019

A private DNA ancestry database that's been used by police to catch criminals is a security risk from which a nation-state could steal DNA data on a million Americans, according to security researchers.

Security flaws in the service, called GEDmatch, not only risk exposing people's genetic health information but could let an adversary such as China or Russia create a powerful biometric database useful for identifying nearly any American from a DNA sample.

GEDMatch, which crowdsources DNA profiles, was created by genealogy enthusiasts to let people search for relatives and is run entirely by volunteers. It shows how a trend toward sharing DNA data online can create privacy risks affecting everyone, even people who don't choose to share their own information.

"You can replace your credit card number, but you can't replace your genome," says Peter Ney, a postdoctoral researcher in computer science at the University of Washington.

Ney, along with professors and DNA security researchers Luis Ceze and Tadayoshi Kohno, described in a report posted online how they developed and tested a novel attack employing DNA data they uploaded to GEDmatch.

Using specially designed DNA profiles, they say, they were able to run searches that let them guess more than 90% of the DNA data of other users.

The founder of GEDmatch, Curtis Rogers, confirmed that the researchers alerted him to the threat during the summer.

"We certainly are concerned about privacy also, and it's good that studies like this are done," says Rogers. "But no matter what you do, there will always be some potential for privacy invasion when you are doing genealogy. Genealogy is a procedure in which you want to compare your information to other people's."

Razib Khan, a genomics researcher who is head of scientific content at Insitome, a service that interprets DNA for consumers, called the new security research a large-scale demonstration of weaknesses already known to enthusiasts.

Khan says he has been aware of efforts to "scrape" GEDmatch, or collect more data than usual, and believes a larger attack to whisk away much of the data could already have occurred. "My guess is that almost certainly it's already been done," he says. "Governments are collecting data on people. You never know what they can use it for."

Asked if there was evidence the database had already faced concerted attacks, scraping, or scanning, Rogers said, "I don't want to get into it."

"Not that I am aware of," he added. "I don't know."

Rogers declined to comment on whether he'd been approached by national security officials about the site.

Crowdsourcing DNA

Rogers started the genealogy service as a way for people to upload DNA test results from services like 23andMe and locate relatives among other users, by comparing their DNA. The crowdsourced database now holds 1.3 million profiles, he says, although some of these are duplicates.

As the site grew, it drew the attention of police investigators. In 2017, police in California announced they had used the database, without Rogers' knowledge, to help identify a murderer known as the Golden State Killer. Police did it by uploading DNA data extracted from crime-scene evidence and comparing it with users' data to identify some of his relatives.

Since then, dozens of murderers and rapists have been identified using GEDmatch. But a privacy debate erupted as well, partly because police had searched users' DNA without their knowledge. In response, Rogers allowed users to opt in or out of police searches, or just delete their profiles.

But there was an even broader concern: if a DNA database is large enough, practically everyone can now be tracked though their relatives, even if they never took a DNA test.

With the million or so profiles in the database, most Americans have second or third cousins in it, says Doc Edge, a researcher at the University of California, Davis, who last week posted the first paper showing how ancestry databases could be vulnerable to a clever searcher.

Read the rest here:

https://www.technologyreview.com/s/614642/dna-database-gedmatch-golden-state-killer-security-risk-hack/

What Your Personal Information is Worth to Cyber-criminals

By Ionut Ilascu, BleepingComputer, October 15, 2019

Cybercriminals have multiple markets to get illicit goods and prices on these underground forums are likely driven by supply and demand, just like in the legal economy.

Offerings found on deep and dark web (DDW) markets include anything that can be monetized in one way or another. Common goods cover any financial information that can be used for bank fraud.

Full info packages

A typical assortment of products and services comprises personally-identifiable information, payment card data, credentials, access to compromised systems, distributed denial-of-service, forged documents, credentials, and access to compromised services.

Many of the underground sites that provided the data are no longer active, some because law enforcement brought them down. Nevertheless, the data is still a good indicator of the value of stolen data to cybercriminals.

Full packages of data that can be used to steal a US victim's identity sell for $4-$10, the researchers say. These are called 'fullz' and include at least the name, Social Security number, date of birth, and account numbers.

The price seems low but it can get as high as $65 when accompanied by financial information, such as credit scores. The better the credit score, the higher the price. A score of 700, for instance, increased the fullz' value to $40.

A better credit score is viewed more favorably by financial institutions, so fraudsters are more likely to succeed in their endeavors. Prices for fullz also depend on the country the victim is based in.

Documents, passports in particular, are more expensive products and sell in three formats: digital scans, templates, and the physical document with the buyer's details.

The last of the three is the priciest and normally come with accompanying documents, like a driver's license. Their price in 2017 was between $2,890 and $5,000, Flashpoint notes.

The price of templates, in PSD format, seems to vary depending on the country, most expensive ones being for Netherlands, $50. However, the value of passport templates for other countries in Europe is close at $45 (France, Germany, Spain).

For the U.S., Flashpoint analysts found a price of $18, which is closer to Canadian and Australian passport templates. The lowest, though, appears to be for Sweden, only $5.

Cards and bank account access

Bank logs, which are essentially access to victims' bank accounts, are also a common find on underground markets. Their value depends directly on the balance.

According to Flashpoint's report today, German bank logs with a EUR 7,000 balance are worth $175, while U.S. ones with $5,000-$10,000 cost around $62.

The reason for this and other discrepancies in pricing these illegal goods is unknown.

Probably the most common offer on DDW markets is payment card data, which can be used to clone cards or make online purchases. The data is stolen either from PoS terminals (dumps) or from online transactions (cards).

Flashpoint estimates "with a moderate degree of confidence in 2019 that the price of cards in card shops likely often ranges between $2 and $20 USD" but it may go as high as $200 in some cases.

Remote access (RDP) to systems is also a popular offer on DDW markets as this accommodates a number of needs: from delivering spam and hiding connections to running account takeover attacks, fraudulent activity, and carding.

The researchers say that sellers have different types of RDP access organized by country, operating system, administrator access, and whether they are residential, hacked, or patched.

Download the free PDF book here:

https://www.bleepingcomputer.com/news/security/what-your-personal-information-is-worth-to-cybercriminals/

Microsoft and NIST partner to create enterprise patching guide

A NIST guide was needed as the patch testing process for some companies involved asking questions on internet forums

By Catalin Cimpanu, ZeroDay, October 11, 2019

Microsoft and the US National Institute of Standards and Technology (NIST) have joined forces to create a NIST guide for applying security patches in the enterprise sector.

The two organizations are now inviting other interested parties to provide input for this new guide. The invitation is valid for vendors, companies, or lone individuals alike.

The result of this work will be a NIST Special Publication 1800 practice guide that system administrators can follow to organize or optimize a company's internal patching procedures.

The guide is expected to have a huge impact since it has the backing of NIST, the US government organization responsible for setting up industry guidelines.

ROOTED IN THE 2017 RANSOMWARE OUTBREAKS

Work on this joint Microsoft-NIST partnership began in 2018, as part of a project named the Critical Cybersecurity Hygiene: Patching the Enterprise Project.

Microsoft played a crucial role in setting it in motion. The company said it began looking into how companies patch their computer fleets after the three ransomware outbreaks of 2017 -- namely WannaCry, NotPetya, and Bad Rabbit.

The OS maker said that many of the organizations that got hit had failed to install patches, even if security updates were available. This led Microsoft to investigate why companies didn't patch their systems.

"A key part of this learning journey was to sit down and listen directly to our customer's challenges," said Mark Simos, Lead Cybersecurity Architect, Cybersecurity Solutions Group at Microsoft.

"Microsoft visited a significant number of customers in person (several of which I personally joined) to share what we learned [...] and to have some really frank and open discussions to learn why organizations really aren't applying security patches," the Microsoft exec said.

COMPANIES APPROACHED PATCHING DIFFERENTLY

These meetings revealed that organizations had very different approaches to patching, and delays in applying security updates occurred as a result.

One of the primary reasons invoked in these meetings was that companies didn't have a patch testing procedure in place, and many were delaying patches in order to make sure bugs or crashes wouldn't cause downtime in production systems.

Simos said that in some organizations, the process of testing a patch "consisted solely of asking whether anyone else had any issues with the patch in an online forum."

Furthermore, some companies also said they also didn't know how fast they should be applying patches, leaving each to interpret and assess the severity of security updates based on their own criteria.

Read the rest here:

https://www.zdnet.com/article/microsoft-and-nist-partner-to-create-enterprise-patching-guide/

Resilient Interdomain Traffic Exchange: NIST Releases Second Public Draft of SP 800-189

Staff, NIST, October 18, 2019

In recent years, numerous routing control plane anomalies such as Border Gateway Protocol (BGP), prefix hijacking, and route leaks have resulted in denial of service (DoS), unwanted data traffic detours, and performance degradation. Large-scale distributed denial of service (DDoS) attacks on servers using spoofed internet protocol (IP) addresses and reflection-amplification in the data plane have caused significant disruption of services and resulting damages.

NIST has released a second public draft of **NIST Special Publication (SP) 800-189, *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation***. This document provides technical guidance and recommendations for technologies that improve the security and robustness of interdomain traffic exchange. Technologies recommended in this document for securing the interdomain routing control traffic include Resource Public Key Infrastructure (RPKI), BGP origin validation (BGP-OV), and prefix filtering. Additionally, technologies recommended for mitigating DoS and DDoS attacks include prevention of IP address spoofing using source address validation with access control lists (ACLs) and unicast Reverse Path Forwarding (uRPF). Other technologies such as remotely triggered black hole (RTBH) filtering, flow specification (Flowspec), and response rate limiting (RRL) are also recommended as part of the overall security mechanisms.

The document is intended to guide information security officers and managers of federal enterprise networks. The guidance also applies to the network services of hosting providers (e.g., cloud-based applications and service hosting) and internet service providers (ISPs) when they are used to support federal IT systems. The guidance may also be useful for enterprise and transit network operators and equipment vendors in general.

The public comment period ends November 15, 2019. See the publication details below for a copy of the document and comments received on the first draft.

NOTE: A call for patent claims is included on page vi of this draft. For additional information, see the Information Technology Laboratory (ITL) Patent Policy--Inclusion of Patents in ITL Publications.

Publication details:

https://csrc.nist.gov/publications/detail/sp/800-189/draft

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.

Come out for a beer or soda and hors d'oeuvres and meet your NCC team. Learn about the NCC and join us as we dedicate time for our community to provide feedback on the NCC in an open forum. This is also an opportunity to meet and connect with like-minded individuals in the local cybersecurity ecosystem.

Details here:

https://nationalcybersecuritycenter.growthzoneapp.com/ap/Events/Register/DLyMj39L

SPECIAL INTEREST GROUPS (SIGS)

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

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

Affinity Groups

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

- Women in Security – **W**[omen]**IS (WIS)**
- Young Professional in Security – **Y**[oung Professionals]**IS (YIS)**
- Educators in Security – **E**[ducators]**IS (EduIS)**
- Executives in Security – **E**[xecutives]**IS (EIS)**

Industry Groups

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

- Finance in Security – **F**[inance]**IS (FIS)**
- Healthcare in Security – **H**[ealthcare]**IS (HIS)**
- Retail in Security – **R**[etail]**IS (RIS)**
- DoD in Security – **D**[oD]**IS (DodIS)**

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

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

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

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

ISSA-COS Scholarship Fund Sponsor—ASPG
https://aspg.com/

ASPG
Advanced Software Products Group, Inc.

Update Your Profile!

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

FBI investigating if attempted 2018 voting app hack was linked to Michigan college course

By Kevin Collier, CNN Politics, October 5, 2019

An attempted hack into a mobile voting app used during the 2018 midterm elections may have been a student's attempt to research security vulnerabilities rather than an attempt to alter any votes, three people familiar with the matter told CNN.

Mike Stuart, the US attorney for the Southern District of West Virginia, revealed at a press conference Tuesday that an FBI investigation "is currently ongoing" after an unsuccessful attempted intrusion into the Voatz app, which West Virginia has used since 2018 to allow overseas and military voters to vote via smartphone. No criminal charges have been filed.

The sources told CNN that the FBI is investigating a person or people who tried to hack the app as a part of a University of Michigan election security course. Michigan is one of the main academic hubs of election security research in the country, housing the trailblazing Michigan Election Security Commission.

The office of West Virginia Secretary of State Mac Warner had previously communicated to Stuart that suspicious activity against the Voatz app came from IP addresses associated with the University of Michigan, one of the people familiar with the matter told CNN.

"During the 2018 election cycle, Secretary of State Warner referred to my office what he perceived to be an attempted intrusion by an outside party into the West Virginia military mobile voting system," Stuart said in prepared remarks Tuesday. He added that "no legal conclusions whatsoever have been made regarding the conduct of the activity or whether any federal laws were violated."

The FBI declined to comment on the matter, and the West Virginia Secretary of State's office as well as Stuart's office declined to offer further comment. Rick Fitzgerald, a spokesman for the University of Michigan, said he did not "have enough information at this moment to offer any response."

Voatz co-founder and CEO Nimit Sawhney declined to share specifics of the attempted hack but told CNN Tuesday that it was the only incident from the 2018 election that felt severe enough to turn over to the FBI.

"We stopped them, caught them and reported them to the authorities," Sawhney told CNN Tuesday.

The FBI inquiry stemmed from a particular incident in the Michigan course, where students examined current and proposed mobile voting technology but were instructed not to meddle in existing election infrastructure, according to a person familiar with the matter. This spring, one of the students emailed their professors to say the FBI had obtained a search warrant for their phone, one of the people familiar with the matter said.

The matter highlights one of the most contentious issues in cybersecurity research: One of the best ways to find potential vulnerabilities in software is to have a researcher try to think like a hacker and try to break in. But the US' primary hacking law, the Computer Fraud and Abuse Act, is strict and carries strong penalties for someone found to have gained "unauthorized access" to a system.

West Virginia is the only state that currently uses the system and proponents of Voatz, like Warner, say that the app provides a solution to low voter participation rates among military and overseas voters, that it has passed some security tests and maintain there is no evidence hackers have changed any votes.

"Voatz has been so reluctant to have anyone inspect their system or even disclose the audits of their product that have been conducted," said Joseph Lorenzo Hall, the chief technologist of the Center for Democracy & Technology.

"They are completely opaque, and that is the exact opposite of what a cutting-edge security product used for government elections should be," Hall told CNN. "This gives the technical community zero confidence in their product or operations."

"Election systems are critical infrastructure," Sawhney said. "If you are not an authorized voter, (and) you want to experiment with the system, there are alternate approaches available."

Read the rest here:

https://edition.cnn.com/2019/10/04/politics/fbi-voting-app-hack-investigation/index.html

2019 Schedule of Events

Chapter Meetings – Dinner

Tuesday, November 19, 2019

Chapter Meetings – Lunch

Wednesday, November 20, 2019

Board Meeting

Tuesday, December 3rd at L3Harris from 6-8:00 PM

Mini-Seminars

Saturday, November 16, 2019

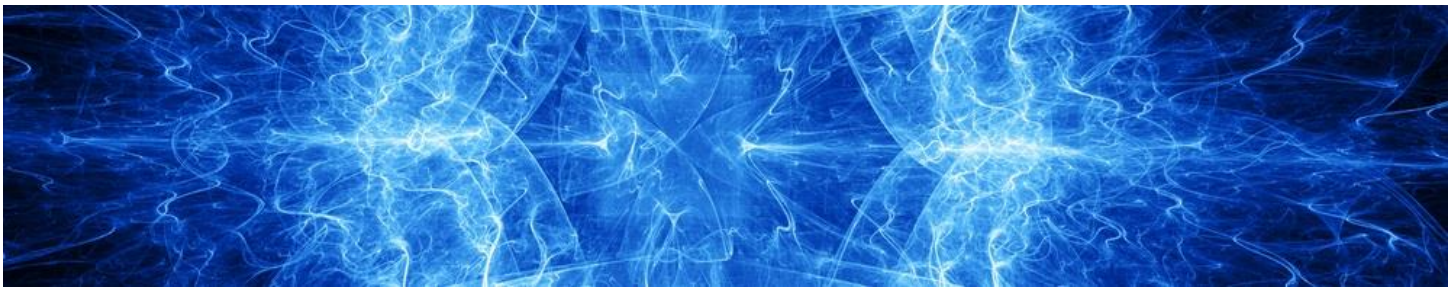
Annual Award Ceremony

Thursday, December 5, 2019

SCP Hotel

2850 South Circle Drive

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



From the Mentorship Team

ISSA-COS Mentorship is available as an embedded feature/service which is matrixed through each SIG. This custom-tailors ISSA-COS Mentorship so that it tailor-fits each career lifecycle stage and special interest. ISSA Mentors and Proteges aren't enrolled into a mentorship program; rather, the process is that of an intake in which a need is assessed with the goal of the need being met. The need is taken in and evaluated and an action plan is created to meet the need. (As an additional need arises, an additional intake is created.)

ISSA Mentorship is an exchange in which both parties are protected and respected. Healthy boundaries are maintained and proprietary knowledge is protected. ISSA Mentorship is designed to be a win-win situation in which both parties are enriched.

ISSA Mentorship is goal/need-driven. The ISSA-COS Mentorship Intake Form serves as a guide regarding the length of the mentorship session as the goal/need of the mentor or protege will determine parameters. The carefully-crafted intake form provides ISSA-COS leadership with metrics so that ISSA Mentorship is treated as a service with KPIs (Key Performance Indicators) and next step suggestions. If ISSA-COS Mentorship can *measurably* boost the careers of its membership, ISSA will, in turn, be boosted as we become known for building each other.

Mentorship Intake Form

email completed form to: mentorship@issa-cos.org

Information Systems Security Association
Colorado Springs Chapter

I seek to:

- ❑ mentor
- ❑ protégé
- ❑ peer-to-peer

I aim to meet:

- ❑ in person
- ❑ by phone
- ❑ via email
- ❑ via Skype

What drives you to invest in mentorship now? Please state two goals:_____

_____

_____

_____

_____

_____

Name:_____

Phone:_____

Email:

_____

_____

Checkmark your current status in the ISSA Cyber Security Career Lifecycle:

Are you on LinkedIn? Y / N
Are you on Skype? Y / N

Have you visited the ISSA-COS website? Y / N

Which ISSA committees or special interest groups align with your interests?

- ❑ Speakers Bureau
- ❑ Friends of Authors
- ❑ Women in Security
- ❑ Healthcare in Security
- ❑ Finance in Security
- ❑ Retail in Security
- ❑ DoD in Security
- ❑ Executives in Security
- ❑ Young Professionals in Security
- ❑ certification prep
- ❑ continuing education
- ❑ other: _____

My mentorship goals align most closely with:

- ❑ career advice
- ❑ building an alliance
- ❑ seeking opportunity
- ❑ technical training
- ❑ practice leadership
- ❑ practice speaking
- ❑ practice authoring for publications
- ❑ solving a specific technical challenge
- ❑ finding my place in our ISSA chapter
- ❑ other _____

MENTOR USE ONLY

Feedback / Recommendations

Time invested:____ mins / hrs

Were goals met? Y / N

Is additional mentorship requested at this time? Y / N

Additional notes:

OFFICE USE ONLY

Follow-up Plan

- ❑ *time recorded*
- ❑ *goals recorded*
- ❑ *resources provided*
- ❑ *referred to SIG:* _____

Next steps:

Ransomware victim hacks attacker, turning the tables by stealing decryption keys

(ISSA-COS Newsletter Editor's note: Whether or not this should be done has been a continuing item of debate as long as I have been publishing this newsletter. ISSA-COS is not recommending that you do this.)

By Graham Cluley, The State of Security, October 9, 2019

Normally it works like this.

Someone gets infected by ransomware, and then they pay the ransom. The victim then licks their wounds and hopefully learns something from the experience.

And that's what happened to Tobias Frömel, a German developer and web designer who found himself paying a Bitcoin ransom of 670 Euros (US $735) after his QNAP NAS drive was hit by the Muhstik ransomware.

However, Frömel didn't just put down the whole unpleasant episode to experience, vow to better protect his devices and employ a more reliable backup regime in future.

No, Frömel decided to hack the very people responsible for the attack.

After decrypting his own data, Frömel (who also calls himself "battleck" online) analyzed the ransomware that had infected his NAS drive, determined how it worked, "hacked back" and stole the criminal's "whole database with keys."

From the sound of things, whoever was behind the Muhstik attack was more successful at writing ransomware than securing their own database from a web developer.

In a posting on the *Bleeping Computing* forum, Frömel admitted what he had done and posted a link to a Pastebin page where he had published the stolen keys as well as the decryption software.

Furthermore, in an attempt to do some good–and deprive cybercriminals of income–Frömel has been seeking out Muhstik victims on Twitter and pointing them towards his decryption keys and instructions on how to recover their data.

Although many may feel tempted to applaud what Frömel did, hacking online criminals is not to be recommended. Frömel himself acknowledges that what he did was against the law, although I would be surprised if he gets into any trouble over it:

Read the rest here:

https://www.tripwire.com/state-of-security/featured/ransomware-victim-hacks-attacker-stealing-decryption-keys/

Answers to Cybersecurity Jeopardy

Types of encryption

1. What is "Asymmetric" encryption
2. What is "Symmetric" encryption
3. What is "Asymmetric" encryption
4. What is "Symmetric" encryption

Identity and Access Management

1. What are "Physical" controls
2. What is "Something you are"
3. What is "Kerberos"
4. What is "RADIUS"

And for Final Jeopardy:

He was the original host of Jeopardy from March 30, 1964, to January 3, 1975 and again from October 2, 1978, to March 2, 1979.

Who is…?

Google's 'Quantum Supremacy' Isn't the End of Encryption

By Tim Simonite, Wired, September 24, 2019

Google accidentally made computer science history last week. In recent years the company has been part of an intensifying competition with rivals such as IBM and Intel to develop quantum computers, which promise immense power on some problems by tapping into quantum physics. The search company has attempted to stand out by claiming its prototype quantum processors were close to demonstrating "quantum supremacy," an evocative phrase referring to an experiment in which a quantum computer outperforms a classical one. One of Google's lead researchers predicted the company would reach that milestone in 2017.

Friday, news slipped out that Google had reached the milestone. The *Financial Times* drew notice to a draft research paper that had been quietly posted to a NASA website in which Google researchers describe achieving quantum supremacy. Within hours, Democratic presidential candidate Andrew Yang was warning that Google's quantum computers could break encryption, and quantum computing researchers were trying to assure the world that conventional computers and security are not obsolete.

Experts are impressed with Google's feat. John Preskill, a Caltech professor who coined the term "quantum supremacy" in 2011, calls it a "truly impressive achievement in experimental physics." But he and other experts, and even Google's own paper, caution that the result doesn't mean quantum computers are ready for practical work.

"The problem their machine solves with astounding speed has been very carefully chosen just for the purpose of demonstrating the quantum computer's superiority," Preskill says. It's unclear how long it will take quantum computers to become commercially useful; breaking encryption—a theorized use for the technology—remains a distant hope. "That's still many years out," says Jonathan Dowling, a professor at Louisiana State University.

Google's conventional computers may have outed the work of its quantum computers. Dowling says he and other researchers got word of the claimed breakthrough last week after a Google Scholar alert pointed them to the draft paper. The company is collaborating with NASA, which may have posted it as part of a pre-publication review process. Google declined to comment. NASA did not respond to a request for comment.

Google and others are working on quantum computers because they promise to make trivial certain problems that take impractically long on conventional computers. The approach seeks to harness the math underpinning quantum mechanical oddities such as how photons can appear to act like both waves and particles simultaneously. In the 1990s, researchers showed this could provide a powerful new way to crunch numbers. Interest in the field spiked after a Bell Labs researcher authored an algorithm that a quantum computer could use to break long encryption keys, showing how the technology might leapfrog conventional machines.

More recently, academic and corporate researchers have built prototype quantum processors and touted use cases in chemistry and machine learning. Those devices can work on data today, but they remain too small and error-prone to challenge conventional computers for practical work. Preskill coined the term quantum supremacy in a 2011 talk considering how researchers could prove quantum hardware did in fact offer benefits over classical computers.

Google, IBM, Intel, Microsoft, and several startups have boosted investment in quantum computing significantly since then. That's made the moment of quantum supremacy feel inevitable. "This is something we expected maybe sooner than later," Dowling says.

One reason for that expectation was Google's own researchers saying as much. In 2017, John Martinis, who leads the company's quantum hardware research, predicted his team would achieve supremacy by the end of that year. Google, IBM, and Intel have all displayed quantum processors with around 50 qubits, devices that are the building blocks of quantum computers, around the size experts expected would be needed to demonstrate quantum supremacy.

Qubits represent digital data in the form of 1s and 0s just like the bits of a regular computer. The power of a quantum processor comes from how qubits can also attain a state called superposition that represents a complex, and frankly confusing, combination of both 1 and 0.

Superposition allows a collection of qubits on a quantum processor to do much more than an equivalent number of conventional bits, at least on some problems. As you add more qubits, the possible combinations increase exponentially. At around 50 qubits, it becomes difficult for even the largest supercomputer to simulate what the qubits can do.

That phenomenon underpins Google's supremacy experiment. Its researchers challenged a quantum processor called Sycamore, with 54 qubits, to sample the output from a quantum random number generator. They set a version of the same challenge to some powerful Google server clusters, as well as to the Summit supercomputer at Oak Ridge National Lab, the world's fastest since it was powered on last year.

Read the rest here:

https://www.wired.com/story/googles-quantum-supremacy-isnt-end-encryption/?utm_brand=wired-science&utm_medium=social&utm_social-type=owned&mbid=social_tw_sci&utm_source=twitter

ISSA Photos are courtesy of our Chapter Photographer
Warren Pearce

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


ISSA


ISSA


Insomniac

WWW.ISSA-COS.ORG

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

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

Article for the Newsletter?

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

Send your article ideas to the Newsletter at:

newsletter@issa-cos.org

Chapter Officers:

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

Recorder/Historian: Andrea Heinz
- Deputy: **Vacant**

Dir. of Professional Outreach: Katie Martin
- Deputy: **Vacant**

Director of Communications : Christine Mack
- Deputy: Ryan Evan

Director of Certifications: Derick Lopez
- Deputy: Luke Walcher

Vice President of Membership: David Reed
- Deputy: Melissa Absher

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

Member at Large: Bill Blake
Member at Large: Jim Blake
Member at Large: James Asimah
Member at Large: Dennis Kater

Committee Chairs:

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

Executive Assistant: Andrea Heinz

** Executive Board Members*

Past Senior Leadership

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

Former coder blows his logic bomb guilty plea deal in court

By Kieren McCarthy, The Register, June 25, 2019

A programmer facing up to 10 years in the cooler, and as much as $250,000 in fines, blew his guilty plea deal on Monday – after he tried to avoid admitting full blame for his actions.

David Tinley, 62, was in court to admit planting logic bombs [PDF] in spreadsheets he had developed for Siemens over a decade ago: if he pleaded guilty early and avoided a full-blown trial, the US justice system would cut him a deal resulting in a lesser sentence.

At the last minute, however, Tinley tried to push a more innocent explanation for his actions.

Read the rest here:

https://www.theregister.co.uk/2019/06/25/siemens_logic_bomb/

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