Happy New Year to you all!

Colleagues,

We are off to a fast start in 2015, and I want to ensure we keep everyone informed. We had a really good January meeting and appreciated having TVAR Solutions and Nimble Storage serve as our sponsor for the month. Because of our great turnout, they shared what a wonderful organization COS-ISSA is with their colleagues, and CA Technologies has stepped up to sponsor our February meetings. I don't have to tell you all how important it is for an organization like ours to have corporate sponsors, and I really appreciate the great turnout and support we show our sponsors. Let's make sure our Feb lunch and dinner meetings are well attended so we can maintain this momentum that we have going.

In March we have our 2nd Cyber Focus Day at UCCS. This year we are focusing on Cyber Crime and trying to get speakers and vendors to support us on a large scale. The event is FREE for all attendees so share the word with everyone you know and go to www.fbcinc.com/cfd to sign up.

In April we will host a Professional Networking/Business Social event. If you have a catchy name for it please let us know. We're just starting to plan it, but it will be a relaxed environment with finger foods, beer, wine, etc., where you can come out and speak to other members you may not always get a chance to, listen to a couple short speakers on professional networking topics, share some laughs, etc. We already have companies signing up to sponsor this, and we'll get more information out to you in a few weeks. This will be an event you won't want to miss.

This is lining up to be another

A Note From Our President

By Dr. Patrick Laverty

(Continued on page 3)
Experts Unmask 'Regin' Trojan as NSA Tool

By Marcel Rosenbach, Hilmar Schmunt and Christian Stöcker, Der Spiegel, January 27, 2015

Earlier this month, SPIEGEL International published an article based on the trove of documents made available by whistleblower Edward Snowden describing the increasingly complex digital weapons being developed by intelligence services in the US and elsewhere. Concurrently, several documents were published as well as the source code of a sample malware program called QWERTY found in the Snowden archive.

For most readers, that source code was little more than 11 pages of impenetrable columns of seemingly random characters. But experts with the Russian IT security company Kaspersky compared the code with malware programs they have on file. What they found were clear similarities with an elaborate cyber-weapon that has been making international headlines since November of last year.

Last fall, Kaspersky and the US security company Symantec both reported for the first time the discovery of a cyber-weapon system which they christened "Regin". According to Kaspersky, the malware had already been in circulation for 10 years and had been deployed against targets in at least 14 countries, including Germany, Belgium and Brazil but also India and Indonesia.

Symantec spoke of a "highly complex" threat. Many of the targets were in the telecommunications sector, but others included energy companies and airlines. Both Symantec and Kaspersky did not shy away from superlatives when describing the malware program, calling it a "top-tier espionage tool" and the most dangerous cyber-weapon since Stuxnet, the notorious malware program used to attack the Iranian nuclear program.

"We are certain that we are looking at the keylogger-module from Regin," Costin Raiu, head of research for Kaspersky, said of the code published by SPIEGEL. A keylogger is a program that can record keys struck on a keyboard -- thus logging sensitive information such as passwords, email addresses and text documents -- and then send that information back to the malware programmer.

"Pursuant to our technical analysis, QWERTY is identical with the Regin plug-in 50251," Raiu says. In addition, the analysis revealed that Regin is apparently an attack platform that can be used by several different institutions in several different countries. Kaspersky published its findings in a blog post on Tuesday.

The new analysis provides clear proof that Regin is in fact the cyber-attack platform belonging to the Five Eyes alliance, which includes the US, Britain, Canada, Australia and New Zealand. Neither Kaspersky nor Symantec commented directly on the likely creator of Regin. But there can be little room left for doubt regarding the malware's origin.

The source code excerpt published by SPIEGEL comes straight from the Snowden archive.

Regin was also apparently involved in the attack on the Belgian telecommunications firm Belgacom. And Belgacom, as SPIEGEL reported in the summer of 2013, was a target of the British intelligence agency GCHQ. Ronald Prins, head of the Dutch security company Fox IT, which analyzed the attack on Belgacom, told SPIEGEL ONLINE in the summer of 2011 that Regin appeared to be a tool belonging to the NSA and GCHQ.

There are also additional clues pointing to Regin being a Five Eyes tool:

In the QWERTY code, there are numerous references to cricket, a sport that enjoys extreme popularity in the Commonwealth.

There are many similarities with the cyber-weapons system that the intelligence agencies call "Warriorpride" in the Snowden documents.

The targets thus far known are consistent with Five Eyes surveillance targets as outlined in the Snowden documents.

In the last several years, Regin has been exposed as the cyber-weapon behind a number of digital attacks:

We've been getting some good feedback about our fledgling student mentorship program. UCCS has started back up again and we're linking up with our students as everyone starts to settle into their new schedules. We still have room for more students and additional mentors. Anyone interested should contact Melissa or Dave. Thank you to all who are participating.

We do a pretty good job of publicizing job openings. However, we don't often see part-time opportunities or internships. A lot of students have expressed interest in those types of opportunities. If any of your companies have internships and part-time jobs, please forward them to Melissa or Dave so we can get them out to our student members.

The board is currently looking at ways to expand membership participation through additional committees and roles. This will positively impact the chapter in a couple of ways. First, it will provide some additional and/or different services to our members. Second, it will give members some new ways to contribute to the chapter. That will significantly help justify Senior Member and Fellow submissions.

Two new committees have been started: Ethics and Marketing. The chair for the Ethics committee is Tim Westland; more information on additional members of this committee will be forthcoming soon. The chair for the Marketing committee is Suzanne Chance. Please contact her at marketing@issa-cos.org if you're interested in participating in this effort. When accepting position of chairperson, Suzanne stated: “I would love to hear suggestions from members for ideas, contacts, and their opinions of the most vital and immediate directions for the Marketing Committee to pursue. I will try to make both the February lunch and dinner meetings. It is always better to have a wealth of suggestions, especially at the beginning but also along the way, in order to chart a wise course and to avoid as much as possible wasting money and effort. Volunteers are our most precious commodities and are not to be wasted or abused. I look forward to hearing ideas from all members.”

Last, and of course not least, I'd like to welcome those 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.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

A Note From Our President

very busy year for our chapter, but what I hope you are seeing is a concerted effort from your chapter board to meet your professional needs. We are sacrificing hours and time with our families and other things we could be doing, because we believe in you, and we believe that an organization such as ours can have a positive impact on our members’ lives, both professionally and personally. If you have any ideas or have a couple hours a month to help we always need another hand. Thanks much!

Cheers!

Pat
What are your goals for 2015? Are there any certifications in your New Year’s resolutions? Did you know the Security+ exam criteria changed as of 1 Jan 2015? Did you know the CISSP exam criteria will change later this year? Are you ready for these changes? The Training Team is updating the Exam Prep Review Seminar material to incorporate the CompTIA and (ISC)2 changes and we’re also pursuing other initiatives that members have expressed interest in.

**Security+**

The updated Security+ Exam Prep Review Seminar is tentatively scheduled for 11 April, 11 July, and 17 October this year. The cost for this one-day seminar is only $25, so it’s a great way to get certified! CompTIA’s new 401 version of the Security+ exam is significantly different than the previous 301 version. Per CompTIA: “The Security+ exam covers the most important foundational principles for securing a network and managing risk. Access control, identity management and cryptography are important topics on the exam, as well as selection of appropriate mitigation and deterrent techniques to address network attacks and vulnerabilities. Security concerns associated with cloud computing, BYOD and SCADA are addressed in the SY0-401 exam.” If you already hold the Security+ certification, consider attending a Security+ Exam Prep Review Seminar for an update and for CEUs.

**CISSP**

The updated CISSP Exam Prep Review Seminar is tentatively scheduled for August-September this year. The cost for this seminar is $125 for ISSA-COS members. The CISSP Exam Prep Review Seminar will cover the material (ISC)² has reorganized into eight new domains. According to (ISC)², “refreshed technical content has been added to the official (ISC)² CISSP CBK to reflect the most current topics in the information security industry today. Some topics have been expanded (e.g. asset security, security assessment and testing), while other topics have been realigned under different domains.” If you’re thinking about pursuing the CISSP certification, make sure you get the new Candidate Information Bulletin (CIB) from the (ISC)² website. If you already hold the CISSP certification, consider attending the CISSP Exam Prep Review Seminar for an update and for CPEs.

**Study Groups**

We’re starting organized study groups for those who may be interested in obtaining other certifications. A study group is being formed for the Certified Authorization Professional (CAP) certification and another study group is being formed for the CISSP concentration, Information Systems Security Architecture Professional (ISSAP). Additional study groups can be organized for other certifications if there are enough members interested.

**Instructors**

Looking for a volunteer opportunity? Looking for a way to share your knowledge/expertise? We’re always looking for instructors for both the Security+ Exam Prep Review Seminar and the CISSP Exam Prep Review Seminar. We provide the slides, but you can modify them as you see fit as long as your changes remain consistent with the official CompTIA (for Security+) and (ISC)² (for CISSP) criteria. Our policy is that Security+ instructors be Security+ certified, and CISSP instructors be CISSP certified.

(Continued on page 5)
Help Wanted

We’re looking for someone to assist with organizing the CISSP Exam Prep Review Seminar this year. Duties include:

- Recruit and schedule instructors
- Coordinate review of course content and accompanying PowerPoint slides
- Coordinate printing of slides and provide to students at each session
- Proctor review sessions
- Coordinate with the ISSA Training Team registrar and refreshments coordinators to communicate class size for planning/preparation purposes
- Help set up classroom for instructors
- Respond to student queries as needed

CEU/CPE Opportunities

Looking for CompTIA Continuing Education Units (CEU)? Looking for (ISC)2 Continuing Professional Education (CPE) opportunities? Consider organizing a study group. Consider volunteering your time with the Security+ Exam Prep Review Seminar. Consider volunteering your time with the CISSP Exam Prep Review Seminar. There are many volunteer opportunities available.

Contact Colleen Murphy (cmurphy.cs@hotmail.com) to volunteer or if you have questions.

We have a lot planned for this year, so stay tuned for updates.

A Note from Our Vice President

2015 has started out to be a busy year with a lot of exciting events. The first meeting was a great success with over 100 people attending. I want to say a big thank you to Russ Weeks, member at large, and Matt Everlove, recorder, for signing everyone in. The board would like to have different members sign people in at the meeting so we all get to know each other. If anyone is interested in volunteering to sign people in at the meetings or events, please send me an email, thombuc@aol.com, with which meeting or event you would like to volunteer for. The only requirement is to be at the meeting a bit early, smile and help people find their names on the sign in sheet. The board will provide the sign in sheets, pins and CPE forms.

We have been asked by TREA to remind everyone to park on the south end of the building. There is also parking on the west side of the building too. The parking on the north side is for the bingo players.

On February 25, CTU is having a Networking Event that ISSA-COS will be part of. This event is for the students at CTU to talk to “vendors” for possible employment or assistance in getting a job. Right now Mark Spencer, Melody Wilson, Dave Reed and myself will be there to talk with these individuals about what ISSA-COS can do for them. Thanks to all who volunteer to be there.

Everyone mark their calendar and sign up for the March 25, Cyber Security Focus event. UCCS will be on spring break so parking will be easier than riding the bus as we did for the October event. More to come as the event agenda is finalized.

Cindy
Our February 2015 Meeting Sponsor

The title of the presentation will be "Layer 7 Cross Domain Solutions and High Assurance Guards" and the presenter will be Col. (Ret.) Dave Gruber. Col Gruber was previously the Chief of IT Procurement at the Pentagon and the GPS Wing Commander.

Wednesday, February 11, 2015 1045 - 1245 & Thursday, February 19, 2015 1745 - 1945

CA Technologies, the world's leading independent IT management software company, helps customers optimize IT for better business results. CA's Enterprise IT Management solutions for mainframe and distributed computing enable "Lean IT" empowering organizations to more effectively govern, manage and secure their IT operations.
Apple iOS Now Targeted In Massive Cyber Espionage Campaign

By Kelly Jackson Higgins, DarkReading, February 4, 2015

An extensive and sophisticated cyber espionage operation targeting mainly Western military, government, defense industry firms, and the media, now has a new weapon: a spyware app for Apple iPhones and iPads.

Operation Pawn Storm, which has been tied to Russia by at least one security research firm, is using a specially crafted iOS app to surreptitiously steal from the mobile device text messages, contact lists, pictures, geo-location information, WiFi status of the device, lists of installed apps and processes -- and to record voice conversations, according to new Trend Micro research.

"The Cold War has returned in cyberspace, and Apple has become the gateway to western elites," says Tom Kellermann, chief cyber security officer with Trend Micro. "Pawn Storm has evolved to now incorporate proximity attacks against Western victims."

Trend Micro researchers, who found the iOS malware while studying and tracking Operation Pawn, say they believe the Apple spyware gets installed on systems already compromised by the attackers. It's similar to the "next-stage" SEDNIT malware they found targeting Microsoft Windows systems.

"We found two malicious iOS applications in Operation Pawn Storm. One is called XAgent (detected as IOS_XAGENT.A) and the other one uses the name of a legitimate iOS game, MadCap (detected as IOS_XAGENT.B). After analysis, we concluded that both are applications related to SEDNIT," wrote Trend mobile threat analysts Lambert Sun and Brooks Hong and senior threat researcher Feike Hacquebord, in a blog post today.

"The obvious goal of the SEDNIT-related spyware is to steal personal data, record audio, make screenshots, and send them to a remote command-and-control (C&C) server. As of this publishing, the C&C server contacted by the iOS malware is live," they said.

When XAgent runs on iOS 7, its icon doesn't show up on the mobile device. It's hard to kill, too: When the researchers attempted to terminate the app's process, it restarted right away. When running on iOS 8, however, the icon is not hidden and doesn't automatically restart after it's killed. The researchers say this shows the malware was created before iOS 8's release in September of last year.

"We can see that the code structure of the malware is very organized. The malware looks carefully maintained and consistently updated," the researchers said.

Operation Pawn Storm cyberattacks have intensified in the wake of US-Russian tensions, and the organizations and regions targeted appear to point to Russia or Russian interests. The attackers are going after the US, NATO allies, and Russian dissidents. Among the targets of some phishing attacks used in the campaign are ACADEMI (the US defense contractor formerly known as Blackwater), SAIC, and the Organization for Security and Cooperation in Europe.

Trend Micro so far has stopped short of attributing the attacks to Russia. Researchers at FireEye, however, recently called out the Russian government as being behind the Operation Pawn Storm campaign--specifically the so-called APT28 hacking group. "This Russian government-backed type of espionage has been very mysterious and hard to nail down over all these years on the Internet," Dan McWhorter, lead researcher for the report and vice president of threat intelligence for FireEye, told Dark Reading in October. "In my opinion after looking at our research, it confirms that yes, in fact, the Russian government is doing this, and it gives us a body of evidence to put against that assertion that wasn't there previously."

Read the rest here:
By Peter Clusky, Irish Times, February 2, 2015

The spies had come without warning. They plied their craft silently, stealing secrets from the world’s most powerful military. They were at work for months before anyone noticed their presence. And when American officials finally detected the thieves, they saw that it was too late. The damage was done.

How is the criminal justice system learning to cope with the unique complexities of digital evidence, with the analysis of mobile phone data, satellite imagery and emails? And that’s before you add in all the potentially sensitive material on social media sites such as Facebook, Twitter, YouTube, Flickr and Instagram.

Advances in forensic science, particularly in DNA analysis, continue to revolutionise the ability of investigators to build conclusive cases.

But, in a world where hacking is increasingly the criminals’ tool of choice, how well-equipped are we to drive cyber investigations in pursuit of crucial evidence?

There are two strands to the answer. The first is that courts have traditionally preferred direct witness evidence to digital data, which is sometimes disallowed as stand-alone evidence, often for fear that it can be tampered with or that such tampering may be difficult or impossible to identify.

Judge training

As a result, there is a mindset to be changed. It begins with judges, who need to be trained in the complexities of digital evidence: how to gather and analyse it, how to authenticate it, and how its veracity or accuracy can be challenged – exactly as courts around the world have always done.

In the US, according to Gary Kessler, associate professor at Embry-Riddle Aeronautical University in Florida, and an academic who has looked at the relationship between the judiciary and digital evidence, most judges acknowledge the need for additional training, particularly in areas such as computer forensics.

While they are “appropriately wary” of digital evidence, says Kessler, they are also professional enough to know they need to be equipped to understand arguments made by lawyers in highly technical cases, by expert witnesses and in previous judgments.

As Kessler points out, even scratching the surface tells us that digital forensics entails high-level familiarity with the concepts of computer architecture, operating systems, software engineering and computer networking together with the rules of evidence as they apply in “cyberlaw”.

Which brings us to the second strand of the answer: that having trained the judiciary, the next stage is constant vigilance when it comes to the handling and forensic examination of digital evidence.

Because it turns out that wary judges are absolutely correct to be wary: digital data is often easily altered, it can be difficult to distinguish between original data and copies, and so extracting, securing and documenting digital evidence needs special expertise and attention.

As the US bible on the subject, Forensic Examination of Digital Evidence: A Guide for Law Enforcement points out, the greatest single challenge facing investigators in the courtroom is demonstrating “that the particular electronic media contained the incriminating evidence”.

In evidence terms, some of the most complex cases in the world are heard by the International Criminal Court (ICC) in The Hague, which tries charges of genocide, crimes against humanity, and war crimes. In many cases the victims number in their thousands or even tens of thousands.

Uhuru Kenyatta

In the recent high-profile case against the Kenyan president, Uhuru Kenyatta, which collapsed in December, issues of evidence and its quality were central.

Each side claimed that the other’s witnesses were unreliable and several had to be withdrawn, leaving the case looking increasingly flimsy, while access to mobile phone records and bank statements were still a key problem for the prosecutor when the charges were thrown out.

A report for the ICC by the Human Rights Centre at Berkeley Law School placed those issues in a wider context when it observed that in 2013 the number of mobile phone subscriptions worldwide was 6.8 billion, up from 6 billion in 2011 and 5.4 billion in 2010.

Read the rest here:
Request for Chapter Presenters

We are looking for members to present at both the lunch and dinner meeting. The presenter has about 40 minutes to give the presentation and answer questions. This could be one slide with a situation identified and audience will then discuss possible solutions or a how-to presentation with a demonstration afterwards. The below listed are topics that have been suggested as areas of interest from our members. Please send an email to either, Pat Laverty (plaverty1961@gmail.com) and/or myself, Cindy Thornburg (thornbuc@aol.com) with topic to be presented, and we will connect with you for your availability. We would like the topic to be presented at both meetings however we do understand that may be difficult to accomplish.

- Cyber Security Laws in Colorado
- Interior Protection
- Building in Resiliency
- Ethics
- Intrusion Detection/Prevention Systems – configuration and how to review
- Making the Business Case for Security – how to
- Hacking – how to
- Application Security Scanning
- COMPTIA CE Cycles & Fee Structure
- A Summary and Rating of available Certifications
- A Survey of current IA Incidents We Should Know About (heartbleed) and What They Mean for the State of Our Industry
- Latest Innovations in Network Management Systems
- Real World Case Studies
- Threat Overview – Real World
- Legal Issues in Information Systems
- Asymmetric Warfare – what is it
- Spear Fishing – what is it and demonstration
- Prevention of Cyber Bullying
- Best Practices for Backing Up & Archiving Corporate Data
- When to Maximize or Minimize Your Cyber Footprint/Persona
- Threat Structuring
- Security Modeling – how to
- Data Flow Control
- Trusted Software Development – how to
- Risk Management Framework and what does it mean
- Case Study of Breaches – how they happen and how to prevent
- Security Architecture Development – ‘Building it In’
- ‘Mobile’ Security Management
- Bring Your Own Device (BYOD)
- Biometric Security and Privacy
- Hacking Back

Thank you!

Cindy
Join us for the 2nd Annual Information Systems Security Association (ISSA) - Colorado Springs Chapter - Cyber Focus Day (www.fbcinc.com/cfd) set to take on Wednesday, March 25, 2015 at the University of Colorado - Colorado Springs (UCCS).

Subject matter experts will be on hand to brief attendees on the latest trends, best practices, and remediation strategies in cybersecurity and cybercrime. This one-day forum will offer cyber, IT, business, law enforcement, government, military, academic, training, and other professionals a unique, local opportunity to get up-to-date information on rapidly evolving cybersecurity challenges.

This will also be an excellent opportunity to network with peers, and to join the cybersecurity conversation in Colorado Springs.

**NO COST TO ATTEND:**
Attendance for ISSA members, military/government personnel, and contractors (with a .gov or .mil e-mail address) is free. *CPE/CEU Certificates will be available for attendees.

**EXHIBIT, SPONSOR OR SPEAK:**
Presentation sessions are still available and you can showcase your company's capabilities as an exhibitor/sponsor. For more information contact Dennis O'Neill at dennis@fbcinc.com.

Hosted by the Information Systems Security Association – Colorado Springs Chapter: www.issa-soc.org
Sheriffs are campaigning to pressure Google Inc. to turn off a feature on its Waze traffic software that warns drivers when police are nearby. They say one of the technology industry's most popular mobile apps could put officers' lives in danger from would-be police killers who can find where their targets are parked.

Waze, which Google purchased for $966 million in 2013, is a combination of GPS navigation and social networking. Fifty million users in 200 countries turn to the free service for real-time traffic guidance and warnings about nearby congestion, car accidents, speed traps or traffic cameras, construction zones, potholes, stalled vehicles or unsafe weather conditions.

To Sergio Kopelev, a reserve deputy sheriff in Southern California, Waze is also a stalking app for law enforcement.

There are no known connections between any attack on police and Waze, but law enforcers such as Kopelev are concerned it's only a matter of time. They are seeking support among other law enforcement trade groups to pressure Google to disable the police-reporting function.

The emerging policy debate places Google again at the center of an ongoing global debate about public safety, consumer rights and privacy.

Waze users mark police presence on maps without much distinction other than "visible" or "hidden." Users see a police icon, but it's not immediately clear whether police are there for a speed trap, a sobriety check or a lunch break. The police generally are operating in public spaces.

A Waze spokeswoman, Julie Mossler, said the company thinks deeply about safety and security. She said Waze works with the New York Police Department and others around the world by sharing information.

"These relationships keep citizens safe, promote faster emergency response and help alleviate traffic congestion," Mossler said.

Google has a complicated relationship with government and law enforcement. The company worked closely with the Obama administration to defend itself against hacking by China's government, and it is regularly compelled to turn over to police worldwide copies of emails or other information about its customers. Last year, after disclosures that the National Security Agency had illicitly broken into Google's overseas Internet communication lines, Google and other technology companies rolled out encryption for users, which the U.S. government said could hamper law enforcement investigations. Also last year, Google and other companies sued the U.S. to allow them to more fully disclose to customers details about how much information they were required to hand over each year.

Sheriff Mike Brown of Bedford County, Virginia, said the police-reporting feature, which he called the "police stalker," presents a danger to law enforcement.

"The police community needs to coordinate an effort to have the owner, Google, act like the responsible corporate citizen they have always been and remove this feature from the application even before any litigation or statutory action," said Brown, who also serves as the chairman of the National Sheriffs Association technology committee.

Nuala O'Connor, head of the Center for Democracy and Technology, a Washington civil liberties group, said it would not be appropriate for Google to disable the police-reporting feature.

"I do not think it is legitimate to ask a person-to-person communication to cease simply because it reports on publicly visible law enforcement," she said. She said a bigger concern among privacy advocates is how much information about customers Waze shares with law enforcement, since the service necessarily monitors their location continually as long as it's turned on.

Read the rest here:
Richland College Named a National Center of Digital Forensics Academic Excellence

By Richland College, Undated 2014

Richland College (Dallas, TX) recently met the requirements for designation as a National Center of Digital Forensics Academic Excellence (CDFAE), the only institution in Texas and one of only 10 institutions in the nation to earn this distinction.

The CDFAE program develops partnerships between institutions of higher education and the government to establish standards and best practices for digital forensics students, educators, researchers and practitioners, and in doing so creates advancements in digital forensics and increases the number of qualified professionals in the fields of law enforcement, counterintelligence, national defense and legal.

“At Richland College, digital forensics is a science, technology, engineering and mathematics field, meaning we have developed a unique STEM approach with applied research,” said Zoltan Szabo, Richland College computer science faculty. “Our goal is to teach the scientific method to students in this field as it is required by the legal system for evidence production.”

By focusing on the STEM aspect of digital forensics, Richland College’s digital forensics program provides a non-traditional, research-oriented education to its students in this emerging field.

With its CDFAE designation, Richland College is recognized as a school that establishes a common core curriculum, and the designation requires in-course peer reviews of curriculum and practicum within a three-year period. Richland College also provides the opportunity for students to demonstrate their skills and knowledge in digital forensics, thus giving employers the ability to confirm a candidate’s capability to apply his or her knowledge as suitable in the workplace. In addition, this Richland College program has a certifiable path to meet Department of Defense workforce requirements and national cyber education needs with respect to digital forensics, strengthening the bond among academia, government, professional organizations and the industry.

“The field of digital forensics is very rewarding for those who complete the program, as cyber security fields cannot be outsourced, offering great job security to graduates,” Szabo said.

For more information on Richland College’s digital forensics program, visit www.richlandcollege.edu/forensics. For information on CDFAE, visit http://dc3.mil/cyber-training/cdfae.

Did You See It?

Our very own David Willson had an article in the January issue of the ISSA Journal! Check it out!
Obama on Cybersecurity

By Sean Allocca, and Ernie Austin, Forensic Magazine, January 20, 2015

President Obama looked to calm fears in the wake of the high-profile hacks of Sony and Target earlier this year, by hashing out a multi-step plan to “meet the evolving threat of cyber-attacks, combat identity theft, and protect our children’s information,” in his sixth State of the Union address last night.

Revitalizing suggestions he made in his 2011, Obama had previously proposed legislation that would help private companies and government agencies get the tools they need to combat cyber threats. “If we don’t act,” the president said on Tuesday, “we’ll leave our nation and our economy vulnerable.”

Tackling the growing problems of data mining in schools, the Obama administration has proposed legislation to protect school children from companies that seek to sell student information to third party companies. This legislation would ensure that student information collected in the classroom is used for educational purposes only, and not sold and reused in targeted marketing campaigns. Seventy-five companies have already signed the “Student Privacy Pledge,” according to White House officials, committing not to sell student information or use technologies that engage in marketing.

Other legislation hopes to entice private sector companies to voluntarily share consumer information with each other, and the Department of Homeland Security, with the promise of partial liability protection from lawsuits, according to a story by the The National Journal.

However, critics say expanding the reach of government, in the wake of serious concerns over government surveillance and bulk-data collection, Post-Snowden, are premature. Some wonder if ceding more digital surveillance power to government will be able to prevent hacks, like the Sony hack, in the first place.

With a Republican-led Congress, it remains to be seen how many new proposals will gain bipartisan support. Here are the highlights of the Obama administration’s new cybersecurity policies.

Proposed Cybersecurity Measures

Cybersecurity Information Sharing -- The President includes updates to his 2011 Cybersecurity Legislative Proposal calling for better cybersecurity information sharing between the private sector and government, and it enhances collaboration and information sharing amongst the private sector. The legislation also encourages the formation of private-sector led Information Sharing and Analysis Organizations. These organizations would protect the privacy of ordinary citizens while enabling organizations to share information. This proposal compliments and does not to limit existing effective relationships between law enforcement and other federal agencies and the private sector.

Law Enforcement Tools to Combat Cyber Crime -- Proposed provisions would allow for the prosecution of the sale of botnets, would criminalize the overseas sale of stolen U.S. financial information like credit card and bank account numbers, would expand federal law enforcement authority to deter the sale of spyware used to stalk or commit ID theft and would give courts the authority to shut down botnets engaged in distributed denial of service attacks and other criminal activity.

The proposal reaffirms the legality of cybercrime under existing laws written to prosecute organized crime. Updates to the Racketeering Influenced and Corrupt Organizations Act (RICO) would make sure that non-cybercrime and cybercrimes are seen in the same light.

Personal Data Notification & Protection – Proposed legislation would require companies to notify consumers within 30 days of a security breach. This federal standard would take the place of a patchwork of current state laws that are often confusing to consumers, and have become costly for companies doing business across state lines, the president said.

The Student Digital Privacy Act – The new legislation would ensure information collected about students inside the classroom can only be used for educational purposes, and cannot be sold to third parties to use in targeted marketing strategies. “We want to make sure our children are being smart and safe online,” Obama said to the FTC last week. Coupled with Obama’s 2013 Connect ID initiative, which hopes to connect 99 percent of children with high-speed broadband access by 2018, the Digital Privacy Act can utilize the educational power of the Internet, while simultaneously minimizing the dangers, the president said.

Read the rest here: http://www.forensicmag.com/articles/2015/01/obama-cybersecurity?type=headline
Lizard Stesser Runs on Hacked Home Routers

By Brian Krebs, Krebs on Security, January 12, 2015

The online attack service launched late last year by the same criminals who knocked Sony and Microsoft’s gaming networks offline during the holidays is powered mostly by thousands of hacked home Internet routers, KrebsOnSecurity.com has discovered.

Just days after the attacks on Sony and Microsoft, a group of young hoodlums calling themselves the Lizard Squad took responsibility for the attack and announced that the whole thing was merely an elaborate commercial for their new “booter” or “stresser” site — a service designed to help paying customers knock virtually any site or person offline for hours or days at a time. As it turns out, that service draws on Internet bandwidth from hacked home Internet routers around the globe that are protected by little more than factory-default usernames and passwords.

In the first few days of 2015, KrebsOnSecurity was taken offline by a series of large and sustained denial-of-service attacks apparently orchestrated by the Lizard Squad. As I noted in a previous story, the booter service — lizardstresser[dot]su — is hosted at an Internet provider in Bosnia that is home to a large number of malicious and hostile sites.

That provider happens to be on the same “bulletproof” hosting network advertised by “sp3c1alist,” the administrator of the cybercrime forum Darkode. Until a few days ago, Darkode and LizardStresser shared the same Internet address. Interestingly, one of the core members of the Lizard Squad is an individual who goes by the nickname “Sp3c.”

On Jan. 4, KrebsOnSecurity discovered the location of the malware that powers the botnet. Hard-coded inside of that malware was the location of the LizardStresser botnet controller, which happens to be situated in the same small swath Internet address space occupied by the LizardStresser Web site (217.71.50.x)

The malicious code that converts vulnerable systems into stresser bots is a variation on a piece of rather crude malware first documented in November by Russian security firm Dr. Web, but the malware itself appears to date back to early 2014 (Google’s Chrome browser should auto-translate that page; for others, a Google-translated copy of the Dr. Web writeup is here: https://translate.google.com/translate?sl=ru&tl=en&js=y&p=rev=1&hl=en&ie=UTF-8&u=http%3A%2F%2Fvms.drweb.com%2Fvirus%2F%3Fi%3D4242198&edit-text=).

As we can see in that writeup, in addition to turning the infected host into attack zombies, the malicious code uses the infected system to scan the Internet for additional devices that also allow access via factory default credentials, such as “admin/admin,” or “root/12345”. In this way, each infected host is constantly trying to spread the infection to new home routers and other devices accepting incoming connections with default credentials.

The botnet is not made entirely of home routers; some of the infected hosts appear to be commercial routers at universities and companies, and there are undoubtedly other devices involved. The preponderance of routers represented in the botnet probably has to do with the way that the botnet spreads and scans for new potential hosts. But there is no reason the malware couldn’t spread to a wide range of devices powered by the Linux operating system, including desktop servers and Internet-connected cameras.

KrebsOnSecurity had extensive help on this project from a team of security researchers who have been working closely with law enforcement officials investigating the LizardSquad. Those researchers, however, asked to remain anonymous in this story. The researchers who assisted on this project are working with law enforcement officials and ISPs to get the infected systems taken offline.

This is not the first time members of LizardSquad have built a botnet. Shortly after their attack on Sony and Microsoft, the group’s members came up with the brilliant idea to mess with the Tor network, an anonymity system that bounces users’ connections between multiple networks around the world, encrypting the communications at every step of the way. Their plan was to set up many hundreds of servers to act as Tor relays, and somehow use that access to undermine the integrity of the Tor network.

Read the rest here: http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/
Bitcoin exchange Bitstamp suspends service after security breach

By Shivam Srivastava and Marja Novak, Reuters, January 6, 2015

Bitstamp, one of the largest exchanges for trading the digital bitcoin currency, said it has suspended its service after a security breach on Sunday, resulting in loss of around 19,000 bitcoins.

The breach represented a small fraction of its total bitcoin reserve and the majority was held in secure offline systems, the Slovenia-based firm posted on its website on Tuesday.

Reuters was unable to contact Bitstamp officials in Slovenia or the United Kingdom, but one of the company’s founders, Damijan Merlak, told Slovenian state-owned news agency STA that Bitstamp has enough liquid assets to meet its short-term obligations.

"At present we are setting up a duplicate of the whole infrastructure with experts in San Francisco which should be finished within 24 hours. Then we will be able to resume our services," Merlak told STA.

He said he could not give further details on the breach due to an investigation.

Bitstamp said it believed one of its wallets, which store the digital credentials for a customer’s bitcoin holdings, had been compromised.

Bitstamp said it had notified all customers after learning of the breach, requesting them not to make any deposits to previously issued bitcoin deposit addresses.

"We would like to reassure all Bitstamp customers that their balances held prior to our temporary suspension of services will not be affected and will be honored in full," the exchange said.

Bitcoin, the best-known virtual currency, started circulating in 2009. Unlike conventional money, bitcoin is generated by computers and is independent of control or backing by any government.

Read the rest here:
http://www.reuters.com/article/2015/01/06/us-bitstamp-cybersecurity-idUSKBN0KF0UH20150106

'123456' Maintains the Top Spot on Annual 'Worst Passwords' List

By Splashdata, January 21, 2015

SplashData has announced its annual list of the 25 most common passwords found on the Internet – thus making them the "Worst Passwords" that will expose anybody to being hacked or having their identities stolen. In its fourth annual report, compiled from more than 3.3 million leaked passwords during the year, "123456"and "password" continue to hold the top two spots that they have held each year since the first list in 2011. Other passwords in the top 10 include "qwerty," "dragon" and "football."

As in past years’ lists, simple numerical passwords remain common, with nine of the top 25 passwords on the 2014 list comprised of numbers only.

Passwords appearing for the first time on SplashData’s list include "696969" and "batman."

While Valentine’s Day is less than a month away, "iloveyou" is one of the nine passwords from 2013 to fall off the 2014 list.

According to SplashData, the passwords evaluated for the 2014 list were mostly held by users in North America and Western Europe. In 2014, millions of passwords from Russian accounts were also leaked, but these passwords were not included in the analysis.

SplashData’s list of frequently used passwords shows that many people continue to put themselves at risk by using weak, easily guessable passwords.

"Passwords based on simple patterns on your keyboard remain popular despite how weak they are," said Morgan Slain, CEO of SplashData. "Any password using numbers alone should be avoided, especially sequences. As more websites require stronger passwords or combinations of letters and numbers, longer keyboard patterns are becoming common passwords, and they are still not secure."

Read the rest here:
January Luncheon
ISSA photos are courtesy of our Chapter photographer Warren Pearce.
The Information Systems Security Association (ISSA®) is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

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

Chapter Officers:
President: Pat Laverty
President Emeritus: Dr. George J. Proeller
President Emeritus: Mark Spencer
Executive Vice President: Tim Hoffman
Vice President: Cindy Thornburg
Vice President of Training: Colleen Murphy
Recorder: Matt Everlove
Communication Officer: Jeff Pettorino
Treasurer: Melody Wilson
Member at Large: Russ Weeks
Member at Large: James Asimah
Director of Membership: David Reed
Dir. of Professional Outreach: Chuck Forth

Position Chairs:
David Willson—Sponsorship
Don Creamer—Newsletter

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Can you interview one of the "movers and shakers"? Tell us about it!

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

Send your article ideas to Don Creamer at:
doncreamer-issa@q.com

Ensure that "Newsletter" is in the subject line.
Looking forward to seeing you in print!

Decoding The Internet's Hidden Infrastructure

By Chris Mills, Gizmodo, February 7, 2015

The internet has obviously changed our virtual lives beyond recognition — heck, no-one had 'virtual lives' before the internet — but it's also had a marked, if more subtle impact on our physical surroundings.

Ingrid Burrington's project 'Networks of New York' is an attempt to decode some of the internet infrastructure hiding in plain sight — objects and symbols that fill the urban landscape, but which you probably don't pay attention to (and wouldn't recognize even if you did).

On Burrington's website (and in her book), she details curiosities like the different kind of manholes and handholes you encounter in NYC, not to mention all the different kinds of antennae that live on lampposts and subway platforms. There's also a good beginner's guide to street markings, the innocuous graffiti that gives you a clue to what sort of pipelines might be running below your feet.

Read the rest here:

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