Our first Security+ Exam Prep Review Seminar, held on April 1 and 8, was another huge success—thanks to the exceptional work by Susan Ross and our volunteer instructors. And our second Security+ Seminar kicks off in just a few days! Each of these seminars provides a 12-hour comprehensive review of the CompTIA Security+ exam material. Over 50 students registered for these Seminars!

We held eight membership meetings, in Jan, Feb, Apr, and May, four at lunchtime and four in the evening. If you didn’t make it to our monthly meetings, here’s what you missed so far:

- Airport Security, by Dr. Shawn Murray
- What Constitutes Reasonable Security?, by Mr. David Willson
- Silver Linings in the Cloud, by Mr. Derek Isaacs
- Do I Need an Attorney?: Cyber Legal Landscape, by Mr. David Willson
- Fort Carson Cyber Program, by Ms. Martha Laughman

(Continued on page 4)
Wi-Fi can pass through walls. This fact is easy to take for granted, yet it's the reason we can surf the web using a wireless router located in another room.

However, not all of that microwave radiation makes it to or from our phones, tablets, and laptops. Routers scatter and bounce their signal off objects, illuminating our homes and offices like invisible light bulbs.

Now, German scientists have found a way to exploit this property to take holograms, or 3D photographs, of objects inside of a room - from outside of the room.

“It can basically scan a room with someone’s Wi-Fi transmission,” Philipp Holl, a 23-year-old undergraduate physics student at the Technical University of Munich, told Business Insider.

Holl initially built the device as part of his bachelor thesis with the help of his academic supervisor, Friedemann Reinhard. Later on the two submitted a study about their technique to the journal Physical Review Letters, which published their paper in early May.

Holl says the technology is only in prototype stage at this point, and has limited resolution, but is excited about its promise.

“If there’s a cup of coffee on a table, you may see something is there, but you couldn’t see the shape," Holl says. "But you could make out the shape of a person, or a dog on a couch. Really any object that's more than 4 centimetres in size."

The ability to see through walls using Wi-Fi has been around for years. Some setups can detect home intruders or track moving objects with one or two Wi-Fi antennas. Others use an array of antennas to build two-dimensional images. But Holl says no one has used Wi-Fi to make a 3D hologram of an entire room and the stuff inside of it.

“Our method gives you much better images, since we record much more signal. We scan the whole plane of a room,” he says.

Holl’s method differs from the others in few significant ways.

First, it uses two antennas: one fixed in place, and another that moves. The fixed antenna records a Wi-Fi field's background, or reference, for the spot it’s placed in. Meanwhile, the other antenna is moved by hand to record the same Wi-Fi field from many different points.

“These antennas don't need to be big. They can be very small, like the ones in a smartphone,” Holl says.

Second, both antennas not only record the intensity (or brightness) of a Wi-Fi signal, but also its phase: a property of light that comes from the fact it's a wave. Laser light is all one phase, for example, while an incandescent bulb puts out a mix of different phases of light.

Similar to lasers, Wi-Fi routers emit microwave radiation in one phase.

Finally, the signals from both antennas are simultaneously fed into a computer, and software teases out the differences of intensity and phase “more or less in real-time,” says Holl.

This is where the magic happens: The software builds many two-dimensional images as one antenna is waved around, then stacks them together in a 3D hologram. And because Wi-Fi travels through most walls, those holograms are of objects inside a room.

Holl and Reinhard's first holograms are of a shiny metal cross placed in front of a Wi-Fi router:

The resulting images may not look like much, but they prove the concept works: the moving antenna can capture Wi-Fi shadows and reflections of objects in 3D, right through a wall.

Above is a Wi-Fi hologram of a cross. Holl's technique can capture the WiFi shadow cast by the object (left) through a wall.

The applications for Holl's Wi-Fi holography, he says, are pretty expansive. Adding an array of reference antennas, say, inside of a truck, might help rescue workers detect people in rubble left by an earthquake - or spy agencies see if anyone is home.

Read the rest here: http://www.sciencealert.com/scientists-have-found-a-way-to-photograph-people-through-walls-using-wifi
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.

We are holding relatively steady on our membership—~475 members as of the end of May. Overall, we are maintaining our membership with renewals and new memberships—both general and students/Freemiums. Kudos to everyone who referred a student or general member. Keep those renewals and new members coming in! Remember that for each referral you make, you are entered into the ISSA International quarterly drawing for various prizes.

By emphasizing the Freemium program again I want to ensure everyone is aware that it is now an official ISSA program instead of the pilot program we’ve been working with for the last couple of years. It is no longer showing as a member type when you try to join. Now we issue a code to potential student members that they input on the payment page that cancels out the student membership fees. Eligibility rules governing the program remain the same: Full time students, not fully employed in Cybersecurity, etc. If you are referring a student, please have them contact me and I can confirm their eligibility for Freemium (or not). If they are eligible, I will provide a chapter unique payment code for them to use in the payment block when they join as a “Student” member so they can join for free. Students who don’t meet the Freemium criteria can still enroll as “Student” members, too. However, they will have to pay the current student membership rate of $55. If you know of students who might be eligible, please have them contact me.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

Lockheed Martin bets on blockchain for cybersecurity

By Luke Lancaster, C|Net, May 2, 2017

Lockheed Martin has contracted Guardtime Federal to provide blockchain cyber security, the defense company announced in a blog post.

It’s the first US defense contractor to adopt blockchain as part of its security approach and Lockheed Martin says the partnership will allow it to “realize more efficient and secure software development and supply chain risk management.”

A blockchain is a type of secure database that maintains a constantly expanding list of records. Each record, or block, contains a link to a previous block. This makes them inherently resistant to modification by outside sources.

“These new cyber security approaches will enhance data integrity, speed problem discovery and mitigation,” said Ron Bessire, Lockheed Martin’s Engineering and Technology vice president. “The faster our developers can discover issues, the faster we can deliver.”

Read the rest here:
Vendors approve of NIST password draft

By Ryan Francis, CSO May 9, 2017

A recently released draft of the National Institute of Standards and Technology's (NIST's) digital identity guidelines has met with approval by vendors. The draft guidelines revise password security recommendations and altering many of the standards and best practices security professionals use when forming policies for their companies.

The new framework recommends, among other things:

- **Remove periodic password change requirements**
  There have been multiple studies that have shown requiring frequent password changes to actually be counterproductive to good password security, said Mike Wilson, founder of PasswordPing. NIST said this guideline was suggested because passwords should be changed when a user wants to change it or if there is indication of breach.

- **Drop the algorithmic complexity song and dance**
  No more arbitrary password complexity requirements needing mixtures of upper case letters, symbols and numbers. Like frequent password changes, it’s been shown repeatedly that these types of restrictions often result in worse passwords, Wilson adds. NIST said If a user wants a password that is just emojis they should be allowed. It’s important to note the storage requirements. Salting, hashing, MAC such that if a password file is obtained by an adversary an offline attack is very difficult to complete.

- **Require screening of new passwords against lists of commonly used or compromised passwords**
  One of the best ways to ratchet up the strength of users’ passwords is to screen them against lists of dictionary passwords and known compromised passwords, he said. NIIST adds that dictionary words, user names, repetitive or sequential patterns all should be rejected.

  "All three of these recommendations are things we have been advising for some time now and there are now password strength meters that screen for compromised credentials, not just commonly used passwords," Wilson said. "While it wasn't explicitly mentioned in the new NIST framework, we contend that another important security practice is periodically checking your user credentials against a list of known compromised credentials."

  NIST’s Paul Grassi, one of the authors of the report, noted that many of the above guidelines are now only strong suggestions and are not mandatory yet. The public comment period closed on May 1 and now the draft goes through an internal review process. It is expected to be completed by early to mid summer.

  "We look forward to a day in the near future when technology, culture, and user preference allows these requirements to be more broadly accepted. That said, we reviewed a lot of research in the space and determined that composition and expiration did little for security, while absolutely harming user experience. And bad user experience is a vulnerability in our minds," he said. "We need technology to support this (not all password stores do), so we didn’t want to create requirements that agencies had no chance of meeting due to tech limitations."

  Read the rest here:

  NIST document is here:
Salary Survey Extra: Deep Focus on CompTIA Security+

By CeetMag Staff, Certification Magazine, May 5, 2017

We live in a digital world, and our lives are increasingly tied to computer-based tools and apps. There are massive benefits to us from all of the connectivity and computerization — in terms of convenience alone, for example — but also serious liabilities. And until someone creates a foolproof protection tool, there will be an ongoing need for trained cybersecurity professionals.

There are many different options for those looking to enter the information security field, but one of the most popular is to pursue and achieve the Security+ certification offered by IT industry association CompTIA. We typically hear from a large number of Security+-certified individuals when doing our annual Salary Survey, and 2016 was no exception, with Security+ checking in at No. 62 on our Salary Survey 75 list.

Almost 84 percent of Security+ holders who responded to our survey are from the United States, but we also heard from certificants in 20 other countries: Australia, Brazil, Canada, Czech Republic, Cyprus, Germany, Hungary, Ireland, Italy, Jamaica, Japan, New Zealand, Nigeria, Romania, Russia, Singapore, South Africa, Trinidad and Tobago, United Kingdom, and Zimbabwe.

Among U.S. Security+ holders, the average annual salary in 2016 was an enticing $99,790, with a median annual salary of $101,720. The average annual salary across all countries outside the United States was $64,620, with a median annual salary of $73,330.

As with many cybersecurity certifications, Security+ holders are almost all men — 90.8 percent — but we did hear from a number of women as well. Security+ is popular in many high school IT programs, but we didn’t hear from any certification holders 18 or younger, and just 1.9 percent of respondents are between the ages of 19 and 24, with an additional 17.7 percent checking in somewhere between the ages of 25 and 34. The largest group of those surveyed (35.8 percent) are between the ages of 35 and 44, with 24.8 percent between the ages of 45 and 54, and 18.4 percent between the ages of 55 and 64. Also represented: a small faction of geezers (1.8 percent) between the ages of 65 and 74.

The highest level of education attained by most Security+ holders in the survey is either a bachelor’s degree (37 percent) or master’s degree (32 percent). A few (4.4 percent) rose no further through the educational ranks than to graduate from high school, while similar segments of the crowd claim either technical training (11.1 percent) or an associate’s (two-year) degree (11.4 percent).

An impressive 94.9 percent of surveyed Security+ holders are employed full-time, while 1.7 percent have a part-time schedule, 0.5 percent are students, and 2.9 percent are unemployed. Among those with jobs, 42.4 percent have a standard 40-hour work week, while 45.5 percent work between 41 and 50 hours per week. Just 7.6 percent of respondents work more than 50 hours per week, and a further 3.5 percent work between 31 and 39 hours per week.

Read the rest here:
North Korea's Unit 180, the cyber warfare cell that worries the West

By Ju-min Park and James Pearson, Reuters, May 22, 2017

North Korea's main spy agency has a special cell called Unit 180 that is likely to have launched some of its most daring and successful cyber attacks, according to defectors, officials and internet security experts.

North Korea has been blamed in recent years for a series of online attacks, mostly on financial networks, in the United States, South Korea and over a dozen other countries.

Cyber security researchers have also said they have found technical evidence that could link North Korea with the global WannaCry "ransomware" cyber attack that infected more than 300,000 computers in 150 countries this month. Pyongyang has called the allegation "ridiculous".

The crux of the allegations against North Korea is its connection to a hacking group called Lazarus that is linked to last year's $81 million cyber heist at the Bangladesh central bank and the 2014 attack on Sony's Hollywood studio. The U.S. government has blamed North Korea for the Sony hack and some U.S. officials have said prosecutors are building a case against Pyongyang in the Bangladesh Bank theft.

No conclusive proof has been provided and no criminal charges have yet been filed. North Korea has also denied being behind the Sony and banking attacks.

North Korea is one of the most closed countries in the world and any details of its clandestine operations are difficult to obtain. But experts who study the reclusive country and defectors who have ended up in South Korea or the West have provided some clues.

Kim Heung-kwang, a former computer science professor in North Korea who defected to the South in 2004 and still has sources inside North Korea, said Pyongyang's cyber attacks aimed at raising cash are likely organized by Unit 180, a part of the Reconnaissance General Bureau (RGB), its main overseas intelligence agency.

"Unit 180 is engaged in hacking financial institutions (by) breaching and withdrawing money out of bank accounts," Kim told Reuters. He has previously said that some of his former students have joined North Korea's Strategic Cyber Command, its cyber-army.

"The hackers go overseas to find somewhere with better internet services than North Korea so as not to leave a trace," Kim added. He said it was likely they went under the cover of being employees of trading firms, overseas branches of North Korean companies, or joint ventures in China or Southeast Asia.

James Lewis, a North Korea expert at the Washington-based Center for Strategic and International Studies, said Pyongyang first used hacking as a tool for espionage and then political harassment against South Korean and U.S. targets.

"They changed after Sony by using hacking to support criminal activities to generate hard currency for the regime," he said.

"So far, it's worked as well or better as drugs, counterfeiting, smuggling – all their usual tricks," Lewis said.

The U.S. Department of Defense said in a report submitted to Congress last year that North Korea likely "views cyber as a cost-effective, asymmetric, deniable tool that it can employ with little risk from reprisal attacks, in part because its networks are largely separated from the Internet".

"It is likely to use Internet infrastructure from third-party nations," the report said.

South Korean officials say they have considerable evidence of North Korea's cyber warfare operations.

"North Korea is carrying out cyber attacks through third countries to cover up the origin of the attacks and using their information and communication technology infrastructure," Ahn Chong-ghee, South Korea's vice foreign minister, told Reuters in written comments.

Besides the Bangladesh Bank heist, he said Pyongyang was also suspected in attacks on banks in the Philippines, Vietnam and Poland.

Read the rest here:
Global cyberattack is a warning for 'internet of things'

By Staff, Nikkei Asia Review, May 16, 2017

The current global cyberattack targets weaknesses endemic to modern information technology, exploiting security weaknesses in web-connected devices and the anonymity of the virtual currency bitcoin.

Chief Cabinet Secretary Yoshihide Suga told reporters Monday afternoon he had been told of a number of victims in the country. As of Saturday morning, roughly 2,000 terminals at some 600 Japanese IP addresses had been hit, said a private cybersecurity group, the Japan Computer Emergency Response Team Coordination Center. The damage was expected to spread Monday as the workweek resumed.

One computer was affected at water and sewer services in the city of Kawasaki, Kanagawa Prefecture. A Hitachi group company's appliance-ordering system was halted, preventing transactions with volume retailers, and workers were still trying to bring the system back online as of Monday night.

Elsewhere, attacks on infrastructure and production centers also stood out. A U.K. plant belonging to Japan's Nissan Motor suffered an attack, as did French automaker Renault, which halted work at several plants. British hospitals were forced to call off some procedures due to the strike, and the Spanish telecom Telefonica was hit as well. German railways suffered attacks on electronic arrivals and departures boards, as well as ticket machines.

It was no coincidence that companies and municipalities handling critical infrastructure were hit so heavily. The attackers apparently chose targets that would suffer greatly if they did not recover their data quickly, says analyst Toshio Nawa of Japan's Cyber Defense Institute. Such bodies, he says, are easy to extort because they cannot afford for operations to halt.

The use in infrastructure of connected devices, part of the internet of things, made room for the attack. Rail ticket machines and factory production equipment, for example, are now online and therefore vulnerable.

Production control devices and other equipment are made to match the systems they are used with, so it can be difficult to update them. The attackers targeted systems that still run outdated operating systems such as Microsoft's Windows XP. More users lately are unable to apply the latest security updates due to such issues as software incompatibility, which is something of an alarm bell for the internet of things, says Hiroki Takakura, a professor at the National Institute of Informatics.

This cyberattack came in the form of so-called ransomware, which encrypts users' data, rendering it inaccessible, then displays a message demanding payment in order to restore it. Many of those affected in the past have reportedly paid up.

Ransomware has existed since the 1990s, but became more prevalent last year, spurred by the spread of bitcoin. That virtual currency can be bought with a credit card via a computer program and easily sent digitally. No financial institutions are involved in the transaction, so users are harder to pin down, giving hackers reason to expect they will escape capture.

The attack landed in Europe on Friday afternoon, suggesting it could have been planned to take advantage of the weekend, when it would be harder to respond. Attackers may have counted on victims being impatient to solve the problem that day, said Nawa of the Cyber Defense Institute.

Read the rest here:

Factory Robots Are Easy to Hack, Researchers Show

By Gabriela Vatu, Softpedia, May 3, 2017

Cybersecurity firm Trend Micro has found that numerous factory robots have a weak network security, using simple combinations of username and passwords that couldn't even be changed; others didn't even need a password. Imagine having an email account that doesn't need a password and then expand the implications of that to your personal security to robots that build cars and bikes and so on.

Trend Micro looked at robots from several firms: ABB, Fanuc, Mitsubishi, Kawasaki, and Yaskawa. The research paper indicates that not only do these have poor network security but they aren't faring much better when it comes to software protection either. Some, the researchers said, even ran on outdated software.

Tens of thousands of robots using public IP addresses were discovered, which means they were extremely easy to hack.

Some of these industrial machines can receive commands from operators from afar, from a computer or phone. If the connection linking the two is not secure, hackers could use this vulnerability to hijack the machines.

They even went as far as to film a test on an ABB robot programmed to draw a straight line. Researchers reverse engineered the RobotWare control program and the connected software and had the machine draw a line that was 2 millimeters off. That may seem like a small deed, but when applied to certain products these robots are built to create, the slightest miscalculation can translate into a catastrophe.

Read the rest here:
15 Top-Paying Certifications for 2017

By John Hales, Global Knowledge, LifeLock, Undated

Which certifications should be in your list of credentials based on salary? What’s the next up-and-coming certification? This article will help you answer both questions based on data from Global Knowledge’s 2017 IT Skills and Salary Survey.

The survey was distributed globally, but this article focuses on the United States data and variations exist based on where you work, your years of experience and the type of company you work for, but this is still helpful in deciding where to spend your time and money in earning additional certifications.

To qualify for this year’s list:

- A certification had to have at least 115 survey responses to ensure that the data was statistically valid.

The certification exam had to be available as of the writing of this article.

1. Certified in Risk and Information Systems Control (CRISC)

$131,298

The nonprofit group ISACA, which formerly stood for Information Systems Audit and Control Association, but now is an acronym only, offers and manages the CRISC certification. This certification is designed for IT professionals, project managers and others whose job it is to identify and manage IT and business risks through appropriate Information Systems (IS) controls. The CRISC certification from ISACA, introduced in 2010, covers the entire life cycle, from design to implementation to ongoing maintenance.

Competitiveness factor: More than 20,000 people worldwide have earned this credential, and 96% of those who have earned it keep it current. Because of the demand for professionals with these skills and the relatively small supply of those who have them, CRISC is the highest-paying certification on the list year.

Path to certification: To obtain CRISC certification, you must have at least three years of experience in at least two of the four areas that the certification covers, and you must pass the exam. New for 2017, is that the exam is only offered during three eight-week periods (this year they are May 1 – June 30, August 1 to September 30, and November 1 to December 31) as the CRISC is, and is computer-based and is registered for and available at the same locations making taking the exam more of a challenge.

It also requires at least five years of experience in IS, with at least three of those as a security manager. Your experience must be within the 10 years before taking the exam or five years after passing it, however unlike the CRISC for which there are no exceptions to the experience requirement, there are some alternatives to the experience requirement for this certification. Continuing education credits are required each year to maintain your certification.

Preparing for the exam? Take our CISM Prep Course.

2. Certified Information Security Manager (CISM)

$128,156

ISACA also created and maintains the CISM certification. It’s aimed at management and focuses on security strategy and assessing the systems and policies in place.

Competitiveness factor: More than 32,000 people have been certified since its introduction in 2002, making this a highly sought-after area with a relatively small supply of certified individuals, like the CRISC.

Path to certification: The exam is only offered during the same three eight-week periods (in 2017, they are May 1 – June 30, August 1 to September 30, and November 1 to December 31) as the CRISC is, and is computer-based and is registered for and available at the same locations making taking the exam more of a challenge.

It also requires at least five years of experience in IS, with at least three of those as a security manager. Your experience must be within the 10 years before taking the exam or five years after passing it, however unlike the CRISC for which there are no exceptions to the experience requirement, there are some alternatives to the experience requirement for this certification. Continuing education credits are required each year to maintain your certification.

Preparing for the exam? Take our CISM Prep Course.

3. AWS Certified Solutions Architect – Associate

$125,091

The AWS Certified Solutions Architect Associate-level exam demonstrates an individual’s expertise in designing and deploying scalable systems on AWS. It’s unsurprising to see this certification in this year’s top 15 due to the market need for skilled and certified AWS solutions architects.

This is just the first step to achieving the AWS Certified Solutions Architect – Professional certification. According to this year’s salary survey responses, each of the five AWS certifications available report an average salary of more than $100,000 (the average among them all is $125,591).

Competitiveness factor: There are more than 10,000 certified individuals, according to Quora which is a very small number given the popularity of the AWS platform, driving up salaries for certified individuals.

Path to certification: To get certified, you need to have some hands-on experience with AWS (they suggest six months or more). The exam is computer based and offered at Kryterion testing centers. You can also take our official Architecture on AWS course and/or the official exam readiness course, both which will help prepare you for the exam.

The AWS Certified Solutions Architect – Associate certification exam addresses a range of topics, including designing on AWS, selecting the appropriate AWS services for a given situation, ingress and egress of data to and from the AWS environment, estimating AWS costs, and identifying cost-control measures.

Read the rest here: https://www.globalknowledge.com/us-en/content/articles/top-paying-certifications
BrickerBot Author Claims He Bricked Two Million Devices

By Catalin Cimpanu, Bleeping Computer, April 21 24, 2017

Just like Wifatch and Hajime, the BrickerBot malware is the work of a vigilante grey-hat, who goes online by the name of Janit0r, a nickname he chose on the Hack Forums discussion boards.

If you're unfamiliar, BrickerBot is a new malware family that was first identified at the start of the month by Radware researchers. The malware made headlines because it was the first threat of its kind that intentionally bricked IoT and networking devices, by rewriting the flash storage space of affected devices with random data.

On Monday, feeling bad that we did not follow through with the same diligence that the tipster had warned us with, we decided to have another look over janit0r's profile.

What we discovered was a user that registered on January 21, 2017, had the forum boards set up to use the Alaska timezone and had made four posts.

Right off the bat, his first post was the most interesting one. In a forum topic discussing a decline in the number of active Mirai bots, Janit0r made the following statement. Remind you, this still almost two months and a half before Radware's BrickerBot discovery.

His second and third posts also came before BrickerBot became public and attested to his skills as a reverse engineer, in a topic he started himself, discussing a security flaw in Dahua 2nd and 3rd generation IP cameras.

The researcher who discovered and made public the flaw, withheld proof-of-concept exploit code for one month, to give Dahua customers time to apply a firmware update. Janit0r showed dissatisfaction with the researcher's action and published exploitation details for that particular bug himself.

His last post was in a topic started by a user who "heard" that BrickerBot's source had leaked. Janit0r's response was quick and to the point.

At this point, we had to confirm that Janit0r was indeed BrickerBot's author and not just some guy bragging on Hack Forums. This is how we spent the next two days, scraping through the Dark Web, underground hacking forums, and getting in contact with a few threat intelligence analysts we knew.

By Wednesday, we didn't manage to find any other clue of Janit0r's existence, or anybody else claiming to be BrickerBot's author, with some solid proof on his side. That's when we just gave up, and launched a desperate tweet, asking BrickerBot's author to reach out.

BrickerBot Author Claims He Bricked Two Million Devices

Anonymous tip leads us to Hack Forums profile

Since BrickerBot's appearance, law enforcement and the infosec community have been on the hunt for new information regarding how BrickerBot operates and who's behind it.

Destructive actions like these caught the attention of authorities. In the US, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an official alert last week, warning companies to disable Telnet and SSH access to their devices and asking owners to change their devices' default factory passwords.

New information surfaced over the Easter weekend when Bleeping Computer received an anonymous tip about the online identity of BrickerBot's creator. The tipster pointed us towards the profile of a Hack Forums user named janit0r.

We ignored the tip at first since Hack Forums is known to attract a crowd of braggadocio hackers, many of whom tend to "embellish" their abilities or knowledge. We expected that that two weeks after BrickerBot's discovery, Hack Forums would be abuzz with people trying to take credit for BrickerBot, but it was strangely silent.

On Monday, feeling bad that we did not follow through with the same diligence that the tipster had warned us with, we decided to have another look over janit0r's profile.

What we discovered was a user that registered on January 21, 2017, had the forum boards set up to use the Alaska timezone and had made four posts.

Right off the bat, his first post was the most interesting one. In a forum topic discussing a decline in the number of active Mirai bots, Janit0r made the following statement. Remind you, this still almost two months and a half before Radware's BrickerBot discovery.

His second and third posts also came before BrickerBot became public and attested to his skills as a reverse engineer, in a topic he started himself, discussing a security flaw in Dahua 2nd and 3rd generation IP cameras.

The researcher who discovered and made public the flaw, withheld proof-of-concept exploit code for one month, to give Dahua customers time to apply a firmware update. Janit0r showed dissatisfaction with the researcher's action and published exploitation details for that particular bug himself.

His last post was in a topic started by a user who "heard" that BrickerBot's source had leaked. Janit0r's response was quick and to the point.

At this point, we had to confirm that Janit0r was indeed BrickerBot's author and not just some guy bragging on Hack Forums. This is how we spent the next two days, scraping through the Dark Web, underground hacking forums, and getting in contact with a few threat intelligence analysts we knew.

By Wednesday, we didn't manage to find any other clue of Janit0r's existence, or anybody else claiming to be BrickerBot's author, with some solid proof on his side. That's when we just gave up, and launched a desperate tweet, asking BrickerBot's author to reach out.

Anonymous tip leads us to Hack Forums profile

Since BrickerBot's appearance, law enforcement and the infosec community have been on the hunt for new information regarding how BrickerBot operates and who's behind it.

Destructive actions like these caught the attention of authorities. In the US, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an official alert last week, warning companies to disable Telnet and SSH access to their devices and asking owners to change their devices' default factory passwords.

New information surfaced over the Easter weekend when Bleeping Computer received an anonymous tip about the online identity of BrickerBot's creator. The tipster pointed us towards the profile of a Hack Forums user named janit0r.

We ignored the tip at first since Hack Forums is known to attract a crowd of braggadocio hackers, many of whom tend to "embellish" their abilities or knowledge. We expected that that two weeks after BrickerBot's discovery, Hack Forums would be abuzz with people trying to take credit for BrickerBot, but it was strangely silent.

On Monday, feeling bad that we did not follow through with the same diligence that the tipster had warned us with, we decided to have another look over janit0r's profile.

What we discovered was a user that registered on January 21, 2017, had the forum boards set up to use the Alaska timezone and had made four posts.

Right off the bat, his first post was the most interesting one. In a forum topic discussing a decline in the number of active Mirai bots, Janit0r made the following statement. Remind you, this still almost two months and a half before Radware's BrickerBot discovery.

His second and third posts also came before BrickerBot became public and attested to his skills as a reverse engineer, in a topic he started himself, discussing a security flaw in Dahua 2nd and 3rd generation IP cameras.

The researcher who discovered and made public the flaw, withheld proof-of-concept exploit code for one month, to give Dahua customers time to apply a firmware update. Janit0r showed dissatisfaction with the researcher's action and published exploitation details for that particular bug himself.

His last post was in a topic started by a user who "heard" that BrickerBot's source had leaked. Janit0r's response was quick and to the point.

At this point, we had to confirm that Janit0r was indeed BrickerBot's author and not just some guy bragging on Hack Forums. This is how we spent the next two days, scraping through the Dark Web, underground hacking forums, and getting in contact with a few threat intelligence analysts we knew.

By Wednesday, we didn't manage to find any other clue of Janit0r's existence, or anybody else claiming to be BrickerBot's author, with some solid proof on his side. That's when we just gave up, and launched a desperate tweet, asking BrickerBot's author to reach out.

Anonymous tip leads us to Hack Forums profile

Since BrickerBot's appearance, law enforcement and the infosec community have been on the hunt for new information regarding how BrickerBot operates and who's behind it.

Destructive actions like these caught the attention of authorities. In the US, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an official alert last week, warning companies to disable Telnet and SSH access to their devices and asking owners to change their devices' default factory passwords.

New information surfaced over the Easter weekend when Bleeping Computer received an anonymous tip about the online identity of BrickerBot's creator. The tipster pointed us towards the profile of a Hack Forums user named janit0r.

We ignored the tip at first since Hack Forums is known to attract a crowd of braggadocio hackers, many of whom tend to "embellish" their abilities or knowledge. We expected that that two weeks after BrickerBot's discovery, Hack Forums would be abuzz with people trying to take credit for BrickerBot, but it was strangely silent.
You Delete Email, Don’t You? You May Want to Delete Email Accounts.

By Staff, LifeLock, March 28, 2017

How many email addresses have you had? I can’t count the number of email accounts I’ve opened in my life. In the past, I was always looking for the next, new thing—and for any technology solution that was better than the one I had. But an old email address, particularly one that you used for any length of time before moving on, can be an identity theft ticking time bomb. Really.

Risky business

How does an old email account put you at risk? Assuming you used it for a while, you likely received a lot of messages—from friends and family, as well as your bank and other places where you had online accounts. Think about what’s in those messages—personal contact information, old credit card and bank statements, and even embarrassing details about you or people you know.

Now, when you opened that old email account, how good were you at coming up with strong passwords? If the account dates back to before the terms “data breach” and “international hackers” became common in news headlines, that password might be something like “123456” or the name of your dog, cat or significant other (now ex?). Any password along these lines is very easy for a hacker to, um, hack. And then, all of that information—personal, financial or embarrassing—could be used to steal your identity, drain your bank account or even blackmail you.

Delete...or maintain

So, do you have old email accounts that you no longer use? If so, consider reviewing them for any messages or attachments you want to save and, then, deleting those accounts. They’re not providing any benefits, and, in the event the account is breached, they could put you at risk.

Do you have old email accounts that you want to keep? Log in and clean them up. Delete emails, chat messages and even profile information. In the event of a breach in the future, the less you have in a breached account, the less likely you’ll be victimized by an identity thief who gains access. Oh, and while you’re logged in, come up with a strong, complex password that you’re not using on any other account.

One account can lead to another

My LifeLock colleague, Joe Gervais, is a cybersecurity expert and “hacker for good.” He notes that if you used an old email account as a password recovery address for other online accounts, anyone who gains access to your email account could request a password reset for those other online accounts and seize control. How would they know what online accounts you have? Maybe from the email account itself!

If you have hundreds or even thousands of email messages in an old email account, you likely have a whole lot of personal data in those messages. It’s probably time to take action.

Read the rest here:
https://lifelockunlocked.com/tips/delete-email-dont-may-want-delete-email-accounts/?cid=em_lifecycledbm_newsletter_2017MayNL_read_more__
An Intelligent Approach to Cure Security Fatigue

By Marc Solomon, Security Week, May 18, 2017

Late last year, a study by the US National Institute of Standards and Technology (NIST) took an in-depth look at a phenomenon called “security fatigue.” Researchers found that a majority of individuals they interviewed (20 to 60 year olds in a variety of jobs and in rural, urban and suburban environments) experience a weariness or reluctance to deal with computer security. Being bombarded every day by an increasing number of warnings and bad news about the latest attack isn’t bolstering their resolve to deal with the bad guys. In fact, they’re feeling a sense of resignation and loss of control. That isn’t to say we should stop the awareness and education, but we need to devise better and easier ways to empower individuals to protect themselves.

We’re seeing security fatigue on the corporate side as well, but with a twist. Organizations are growing weary of the same old stream of promises they’ve heard from security vendors for years. “We’ll help you consolidate dozens of security vendors for more effective and simpler protection.” Or, “We’ll provide a single pane of glass and all your security visibility and management headaches will go away.” But all this talk is just that – talk.

As I’ve discussed before, in the face of rising complexity and scarce resources, organizations are looking to improve their security posture while making the best use of existing security teams and technology. How do more one-off APIs or another management interface that your security staff need to master and deploy help you reach your goals as a security organization? The answer is: they don’t. Organizations need an approach they can act on now.

Most security professionals are having trouble strengthening their defenses in the face of a rapidly evolving threat landscape and feel they are being left behind. This may cause you to think more threat intelligence will help. But organizations typically have more threat intelligence than they know what to do with. They have multiple data feeds, some from commercial sources, some open source, some industry and some from their existing security vendors – each in a different format. On top of that, each point product within their layers of defense has its own intelligence.

More threat data isn’t necessarily the solution – in fact, it will likely add to the data overload. What you need is a single source of truth. I’m not talking about “the great and powerful Oz” from The Wizard of Oz (who we know was a sham), but the ability to curate the intelligence you do have – both external and internal – so that it’s contextualized, relevant and prioritized and available to all from a central repository. Then you have a fighting chance against the bad guys.

To harness the power embedded in disparate sources of threat data requires aggregating it and translating it into a uniform format for analysis and action. You then need to augment and enrich it with additional internal and external threat and event data. By correlating events and associated indicators from inside your environment with external data on indicators, adversaries and their methods, you gain additional and critical context to understand what is relevant and high-priority to your organization. You now have a single source of truth using your existing threat data.

You also need to empower your existing security team to apply that curated threat intelligence for better decisions and action. That’s where collaboration and automation come in. The repository can become a hub for storing threat intelligence. As security teams add comments into the repository and regularly update the data in the repository it becomes embedded in the processes for collaboration and decision making. Integrating that repository into other existing systems – including, but not limited to SIEM, log repositories, ticketing systems, incident response platforms, orchestration and automation tools – will allow the various teams to use the tools and interfaces they already know and trust to act on that intelligence.

Read the rest here:
http://www.securityweek.com/intelligent-approach-cure-security-fatigue
The Colorado Springs ISSA Chapter has over 400 current members. Many of you have been members for several years and may qualify for the ISSA fellow program. The Fellow Program recognizes sustained membership and contributions to the profession. If you think you or another ISSA associate may qualify in the fellow program, please contact Shawn P. Murray at 5871charlois@gmail.com or at 719-362-0666 to coordinate the process. Shawn is the chair of the chapter awards committee and will help you through the steps. Below are some additional details on the ISSA Fellow Program. Qualification information is also presented below:

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

Nominations and applications are accepted on an annual cycle. The current cycle opened December 2, 2016 and applications will be accepted until July 10, 2017, at 5:00pm Eastern Time. Following the application period, there will be a ten week review period followed by the notification and presentation process. Fellows and Distinguished Fellows will be recognized at the 2016 ISSA International Conference. Submissions received after August 1, 2016 will be considered in the following cycle.

Familiarize yourself with the Fellow Program, and the submission guidelines (http://c.ymccdn.com/sites/www.issa.org/resource/resmgr/Fellow_Program/Fellow_Policies_Revised_June.pdf). If you have questions, contact Shawn or The ISSA Fellow Manager (fellow@issa.org) or call 866 349 5818 (US toll free) extension 4082.

To Become a Senior Member

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

- 5 years of ISSA membership and 10 years relevant professional experience
- All Senior Member applications require an endorsement from their home chapter to qualify.

For your convenience, please feel free to use this Senior Member Application Check-list to confirm eligibility and completion of application

To access the Senior Member application go to: https://www.issa.org/?Senior_member_App

For the Senior Member endorsement form go to: https://www.issa.org/?Senior_Mem_Endorse

To Become a Fellow or Distinguished Fellow

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

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

(Continued on page 13)
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.

developing and teaching courses.

- All Fellow applications require a nomination to qualify
  
  To access the Fellow application go to:
  
  https://www.issa.org/?Fellow_App

  To nominate a Fellow go to:
  
  https://www.issa.org/?Fellow_Nom

  To submit a Fellow letter of recommendation go to:
  
  https://www.issa.org/?Fellow_Recommend

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

- All Distinguished Fellow applications require a nomination to qualify.

  To access the Distinguished Fellow application go to:
  
  https://www.issa.org/?Distinguished_Fellow

  To nominate a Distinguished Fellow go to:
  
  https://www.issa.org/?D_Fellow_Nom

  To submit a Distinguished Fellow letter of recommendation go to:
  
  https://www.issa.org/?Fellow_Recommend

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

Shawn P. Murray, Chapter Recorder  
5871charlois@gmail.com, 719-362-0666
Cyber Word Search

BOTS
CHATROOM
CONTROLS
CYBER WARFARE
ENCRYPTION
FILE
FIREWALL
FREQUENT CHANGES
FRIEND
HARDWIRED
ID THEFT
INTRUSION
IPHONE
MALWARE

NETWAR
NETWORK
NIGERIAN SCAM
PHISHING
SPOOFING
STRONG PASSWORDS
SURFING
SUSPICIOUS
TEXT
TROJAN
TROLL
VIRUS
WHACK
Tons of $80,000 entry-level cybersecurity jobs are sitting empty

By Gary Robbins, Los Angeles Times, April 19, 2017

The nation’s colleges and universities are scrambling to add courses to prepare students to fill the huge number of cybersecurity jobs that have arisen because of the exponential growth in hacking worldwide.

The extent of the problem isn’t clear; analysts say the number of job vacancies ranges from 100,000 to 350,000, with as many as 45,000 positions in California.

Ashton Mozano, a cybersecurity professor at the University of San Diego, says there are thousands of $80,000 entry-level jobs available to applicants who have nothing more than an undergraduate degree in computer science or computer engineering.

Analysts are trying to nail down the actual number of openings. But the shortfall is real.

A lot of the blame has been placed on academia for failing to train large numbers of students with targeted skills. Industry and government officials also are being criticized for failing to define their needs more clearly—a key component for helping colleges solve the labor shortage.

Several vocational schools, such as Hack Reactor and General Assembly, have popped up in Los Angeles in recent years to train people for variety of computer programming jobs, and they teach skills that would be beneficial in cybersecurity. UCLA Extension, USC, Cal State Fullerton, Cal State San Bernardino and Loyola Law School, among others, have cybersecurity programs.

The University of San Diego works closely with Circadence Corp., a San Diego company led by Mozano that specializes in the “gamification” of cybersecurity training. Students are exposed to high-resolution videos and graphics that give them a sense of what a real “hack attack” is like. They also use the immersive software to learn how to spot and prevent digital assaults.

Mozano is trying to change the way that students are taught in hopes of drawing larger numbers of people into the field quickly. “Certain academic fields in mathematics and engineering are infamous for presenting material in drab, monotonic, esoteric, non-interactive manners,” he said.

To make matters worse, cybersecurity suffers from an image problem.

The field pays well, but many computer science students would rather create new products and technologies for Apple or Google.

“Computer science is sexy. Cyber isn’t,” said P.K. Agarwal, regional dean of Northeastern University’s Silicon Valley campuses, which teach cybersecurity. The field offers high-stress jobs “where you can get fired if things go wrong, and no one pats you on the back if there were no problems overnight,” he added.

Analysts said the industry needs to jazz things up and highlight job opportunities.

Meanwhile, the staffing shortage is serious enough that “the president should … train 100,000 new cybersecurity practitioners by 2020,” the Commission on Enhancing National Cybersecurity said Dec. 1.

The shortage also means “you’ll see more things like the Tesco attack, which targeted bank accounts [in England], and a greater risk to healthcare records and everyday devices like your phone,” said John Callahan, director of cybersecurity programs at the University of San Diego. “In the digital age, this is potentially the greatest period of risk that consumers have ever faced.”

There’s special concern about ransomware, a type of malicious software that hackers can use to remotely take control of computers, including those in automobiles. In most cases, victims have paid money—sometimes tens of thousands of dollars—to regain control. For example, hackers carried out such an attack against Hollywood Presbyterian Medical Center last year, leading the hospital to pay $17,000 in ransom.

Read the rest here:

GET A JOB!

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

You can also sign-up on the Cyberjoblist.com site for Job Alerts to be notified when a new job listing is posted!
Scientists hoping to get data off old media first need to find a device that can read it and connect to a modern computer (see 'Old media'). But moving files to modern media is just the first step; the next is making sense of its contents, which requires another suite of tools.

When it comes to old hardware, a good place to start may be the local library. The Memory Lab at the Public Library in Washington DC offers a do-it-yourself station that allows people to transfer 3.5-inch floppy data onto modern formats, for instance, and Stanford University Libraries offers a similar resource for 5.25-inch disks. Gavan McCarthy, director of the University of Melbourne’s eScholarship Research Centre in Australia, has what he calls “the Museum of Redundant Technology”, which can handle a range of formats. “If you have the tape, the disk and whatever it can fit into, we’ve got the plugs,” he says.

For a few dollars per disk, conversion service firms, such as FloppyDisk in Lake Forest, California, and RetroFloppy in Cary, North Carolina, can help. So, too, can data-recovery services, which specialize in damaged media. DriveSavers, a data-recovery firm based in Novato, California, has around 20,000 storage devices, the oldest being a Shugart ST-506 hard-disk drive from 1980. Parker used CBL Data Recovery in Toronto, Ontario, which subcontracted with Muller Media Services (now George Blood Audio in Manhasset, New York), to recover his data and paid about US$3,000.

Success depends on the fragility of the media and how it was stored. 5.25-inch disks are easily damaged by oils and pressure, and Iomega Zip disks are unstable. But it’s not just ‘bitrot’, or damage to media themselves, that makes old media unreadable says McCarthy. “The number of machines and the spare parts are falling off incredibly rapidly.” Paper is, ironically, more stable.

People who have the old drives and power cables may be tempted to set up their own do-it-yourself stations, only to find that new computers no longer contain the boards and interfaces required to make the connection. Some old Zip drives, for instance, plugged into a ‘parallel’ (printer) port — an interface that has largely disappeared today. But there are a range of adapters, mainly used by archivists and video-game enthusiasts, that can help. At the top end is the KryoFlux device, developed by the Software Preservation Society, which can transfer floppy-disk data through a USB interface. The KryoFlux Preservation Technology Group in Maidstone, UK, charges private users about $100 for the hardware.

The operating systems on modern computers may also be unable to read files in old formats. Lori Emerson, director of the Media Archaeology Lab at the University of Colorado, Boulder, says that helping a local science museum to recover a mysterious file on a Zip disk depended on finding the right computer (a Power Macintosh 8100 from 1994 running OS 7) to read the file, which turned out to be a library from an old version of the citation manager EndNote.

Read the rest here: http://www.nature.com/news/disks-back-from-the-dead-1.21916
If Loose Lips Sink Ships, What do They do to Enterprise Security?

By Travis Greene, Security Week, April 26, 2017

Over the past month, the movement of the aircraft carrier USS Carl Vinson and her carrier battle group escorts (described as an “armada” by President Trump) toward the Korean peninsula has become a strange and twisted tale. The sometimes concurring and conflicting statements about the ship’s schedule coming from the Department of Defense and the president leaves us wondering whether these statements were intentional disinformation, a misunderstanding or simply a premature communication of an intended ship’s movement.

Having served aboard the USS Carl Vinson in the late 1990s, I can assure you that the World War II slogan, “loose lips sink ships” is still very much a part of Navy life. Crew members aren’t allowed to share precise dates or locations of ship movement with their families as part of operational security (or OPSEC) practices.

Yes, users are the weakest link in security and we’ve all heard of them falling victim to phishing attacks or leaving their laptop on a bus. But some users will share information that seems innocuous, yet can be used by attackers in social engineering attacks, which are easier, lower risk and less costly than many technical exploits. Let’s look at a few examples of not-so-obvious information sharing.

Out-of-office notifications

An email “out of office” message that includes details of when a user will return from vacation can be used to gain the confidence of another employee to share information. The attacker, posing as a co-worker, could convince another employee (indicated in the out-of-office email) that they are under a deadline to complete a report that needs information before the vacationing employee returns.

This exact scenario has been proven by penetration testers such as Kevin Mitnick, who has commented during his trade show presentations that “this con is based on impersonating a user’s circle of trust.”

From a policy perspective, consider allowing out-of-office notifications only for internal employees. The policy may need to be more specific to only those employees with access to sensitive information, while employees in other departments, such as sales or direct customer interaction roles, are not restricted.

Social Media

We put a lot of personal information up on social media, simply because the profile template asks us for it. Information related to your role, job title, projects worked, company history and skills are standard and is often publically accessible. While this information may not be confidential from a corporate perspective, it is a gold mine of information for con artists. Like the out-of-office notifications, this information can contribute to a social engineering attack that establishes credibility for the attacker to gain access to a user’s circle of trust.

While the social media genie is unlikely to return to the bottle, there are privacy settings that can help limit information sharing. If your organization has a social media team, work with them on setting policies and educating your users on the potential risks.

Sharing with press and vendors

Many enterprises have policies against sharing specific security controls and policies outside of the company. Given past experiences in working with customers, I can attest to the difficulty in publicizing success stories, for good reason. But it can be human nature to show off too much when the cameras are rolling.

For example, a crew filming a “top secret” Super Bowl security center in February 2014 exposed the WiFi network’s credentials. In 2015, a French television network, while reporting on its own security incident, actually filmed a staff member in their offices with user names and passwords written down and visible in the background. A cybersecurity startup exposed a California hospital’s network in demonstrations without permission.

Security professionals are probably not going to be on the invitation list for external media events. But they can provide training to communication staff on what to look out for to protect information, especially in the background of publicly available materials.

Counter-intelligence operations

While recent reports indicate that the Carl Vinson to Korea story was not an intentional ruse, it certainly wouldn’t be the first example of disinformation from a government. The parallel in IT security is next-gen honeypots.

Read the rest here:
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.

North Korea's Latest Tablet Computer Has a Catchy Name: iPad

By Adam Clark Estes, Gizmodo, June 2, 2017

Ryonghung, a North Korean technology company, recently announced a new tablet. It looks a lot like the weird, firewalled computers the country has produced in the past, with the addition of one curious new feature: the name. It's called... the iPad.

The new Ryonghung iPad comes with a "a quadcore 1.2 GHZ CPU, 1GB of RAM, an 8GB hard disk, an HDMI cable connection and comes with a keyboard and 'network connection' capabilities," NK News reports.

Read the rest here:
http://gizmodo.com/north-koreas-latest-tablet-computer-has-a-catchy-name-1795651057

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