Due to circumstances somewhat beyond my control there was no issue published in early May. So… this issue combines both the May and June issues.

Now for some housekeeping items.

Please look through the names found on Page 3, and see if your coin is listed. Also, look to see if you know anyone on the list and let them know how they may receive their coin (yes, even if they are no longer with ISSA-COS.)

If you change your e-mail address, please notify ISSA so that when we download the membership list from their site, we'll have the most current one for you. Recently, there have been a few members who have changed their e-mail addresses, and we have no way of finding out what it now is. I try to send out letters to those whose e-mails bounce back, but sometimes those don't even make it. I've already had one letter return because there was no forwarding address. Are they now in the Witness Protection Program? Alas, I shall probably never know.

One of our members did receive his letter from me, but it took quite some time to get forwarded to his new location. He is on a long term work assignment out of the area, and now has a new e-mail address. He contacted me, and we are getting him on track again.

I know that Mark usually has some very nice things to say about this newsletter, but are there suggestions that you have to improve it? Please let me know. There is nothing in this world that cannot be improved, and this newsletter is certainly one of them. So, if you have any ideas, criticisms or whatever, please drop me a note at doncreamer-issa@q.com. Let's talk.

Don Creamer
By Levi Pulkkinen, SEATTLEPI.COM, May 28, 2013

The FBI seized and ran a child pornography service late last year as investigators worked to identify its customers, one Western Washington man allegedly among them.

Following a lengthy investigation, Nebraska-based agents raided the large child pornography service in November hoping to catch users who shared thousands of images showing children being raped, displayed and abused.

The Bureau ran the service for two weeks while attempting to identify more than 5,000 customers, according to a Seattle FBI agent's statements to the court. Court records indicate the site continued to distribute child pornography online while under FBI control; the Seattle-based special agent, a specialist in online crimes against children, detailed the investigation earlier this month in a statement to the court.

The investigation appears to mark a departure for the Bureau and other federal law enforcement agencies aiming to root out child porn purveyors.

Historically, child pornography investigations stem from tips made to law enforcement, interactions with undercover officers posing as customers or reviews of documentation seized during searches of child porn clearinghouses like the one recently raided in Nebraska. While investigators are known to have posed as child porn dealers – a 2011 effort involved targeted emails to suspected pedophiles – it is not apparent that the FBI previously dealt child porn as part of a sting.

The Nebraska investigation is still in its early stages, and, while charges appear to be forthcoming, no one being prosecuted has been publicly tied to the site thus far. Information obtained during the investigation resulted in a search of one Western Washington home, and investigators are presently reviewing computers seized during that April search.

The FBI declined requests to discuss the investigation or investigators' motivations to continue operating the site. Court records indicate investigators hoped to trace customers and were unable to do so through traditional means.

"This remains an ongoing investigation, and local court rules and Department of Justice policy prohibit me from providing more information at this time," said Sandy Breault, spokeswoman for the FBI Omaha Division. "As in any given matter, if charges are filed, they will eventually become a matter of public record."

Named only as "Website A" in an April 10 search warrant affidavit filed by the Seattle-based agent, the child pornography service was described as an online bulletin board with the primary business of advertising and sharing child pornography.

The affidavit was obtained by seattlepi.com earlier in May through a publicly accessible court records system. It has since been sealed.

Agents in the Omaha area seized "Website A" on Nov. 16 and continued to operate it until Dec. 2, monitoring messages from users of the website, the Seattle special agent told the court. The site was shut down Dec. 2.

At the time the service was shuttered it had more than 5,600 users and 24,000 posts, nearly all of which related to child pornography. At least 10,000 photos of children being posed nude, raped or otherwise abused were broadcast through the site.

Writing the court, the special agent recounted the site users' discussions on how to avoid detection by police. One went so far as to publish a lengthy guide on encryption, and protections placed on the service impeded investigators' work.

Read the rest here:

Are You Missing Your Coin?

Here is the list of current and former ISSA members that Deborah Johnson has at least one coin for. Please take a look at the list to see if you know any of these folks. The coins can be picked up in person, by proxy, or she can mail them to folks if they can be located. Deborah’s email address is djohnson@swcp.com and her telephone number is 719-329-4495 (voicemail) if folks want to contact her directly. Thank you!

April 9, Help Net Security – (International) **Malicious HP scan notifications target employees.** Cybercriminals have been spotted using fake Hewlett-Packard (HP) printer notifications with links to malicious sites to infect targets with malware, a variant of past attacks that used attached documents. Source: [http://www.net-security.org/malware_news.php?id=2463](http://www.net-security.org/malware_news.php?id=2463)

April 11, IDG News Service – (International) **Twitter OAuth feature can be abused to hijack accounts, researcher says.** A researcher at Swissquote Bank presented a method where Twitter’s application programming interface (API) could potentially be misused to send Twitter access tokens to attackers for use in social engineering attacks. Source: [http://www.networkworld.com/news/2013/041113-twitter-oauth-feature-can-be-268646.html](http://www.networkworld.com/news/2013/041113-twitter-oauth-feature-can-be-268646.html)

April 15, The H – (International) **Security hole can damage heating systems.** The ecoPower 1.0 central heating and power system manufactured by German company Valiant was found to have a security vulnerability that could allow attackers to remotely access user and technician functions that could be used to damage the system and alter climate control settings. Source: [http://www.h-online.com/security/news/item/Security-hole-can-damage-heating-systems-1842489.html](http://www.h-online.com/security/news/item/Security-hole-can-damage-heating-systems-1842489.html)

April 17, Softpedia – (International) **Bots used to attack Israeli websites on April 7 spread out in 27 countries.** Trend Micro analyzed a distributed denial of service (DDoS) attack by hackers, associated with Anonymous, on Israeli Web sites and found that most of the traffic came from outside Israel and that many IP addresses used in the DDoS attack were in botnets under the control of cybercriminals. Source: [http://news.softpedia.com/news/Bots-Used-to-Attack-Israeli- Websites-on-April-7-Spread-Out-in-27-Countries-346038.shtml](http://news.softpedia.com/news/Bots-Used-to-Attack-Israeli- Websites-on-April-7-Spread-Out-in-27-Countries-346038.shtml)

April 22, Dark Reading – (International) **Report: DDoS attacks getting bigger, faster than ever.** Arbor Networks’ first quarter ATLAS report found that the average speed of distributed denial of service (DDoS) attacks grew to about 1.77 Gbps, and that large attacks exceeding 10 Gbps are increasing. Source: [http://www.darkreading.com/perimeter/report-ddos-attacks-getting-bigger-faster/240153399](http://www.darkreading.com/perimeter/report-ddos-attacks-getting-bigger-faster/240153399)
Wild, unregulated hacker currency gains following

By Raphael Satter, AP, April 11, 2013

LONDON (AP) -- With $600 stuffed in one pocket and a smartphone tucked in the other, Patricio Fink recently struck the kind of deal that's feeding the rise of a new kind of money - a virtual currency whose oscillations have pulled geeks and speculators alike through stomach-churning highs and lows.

The Argentine software developer was dealing in bitcoins - getting an injection of the cybercurrency in exchange for a wad of real greenbacks he handed to a pair of Australian tourists in a Buenos Aires Starbucks. The visitors wanted spending money at black market rates without the risk of getting roughed up in one of the Argentine capital's black market exchanges. Fink wanted to pad his electronic wallet.

In the safety of the coffee shop, the tourists transferred Fink their bitcoins through an app on their smartphone and walked away with the cash.

"It's something that is new," said Fink, 24, who described the deal to The Associated Press over Skype. "And it's working."

It's transactions like these - up to 70,000 of them each day over the past month - that have propelled bitcoins from the world of Internet oddities to the cusp of mainstream use, a remarkable breakthrough for a currency that made its online debut only four years ago.

When they first began pinging across the Internet, bitcoins could buy you almost nothing. Now, there's almost nothing that bitcoins can't buy. From hard drugs to hard currency, songs to survival gear, cars to consumer goods, retailers are rushing to welcome the virtual currency whose unofficial symbol is a dollar-like, double-barred B.

Advocates describe Bitcoin as the foundation stone of a Utopian economy: no borders, no change fees, no closing hours, and no one to tell you what you can and can't do with your money.

Just days ago the total value of bitcoins in circulation hit $2 billion, up from a tiny fraction of that last year. But late Wednesday, Bitcoin crashed, shedding more than 60 percent of its value in the space of a few hours before recouping some of its losses. Critics say the roller coaster currency movements are just another sign that Bitcoin is a bubble waiting to burst.

Read the rest here:
http://ap.stripes.com/dynamic/stories/B/BITCOINS_RISE?SITE=DCSAS&SECTION=HOME&TEMPLATE=DEFAULT

Bitcoin Isn’t the Only Cryptocurrency in Town

By Tom Simonite, MIT Technology Review, April 15, 2013

In recent weeks, the digital currency Bitcoin has soared and then dipped in value, along the way attracting more public attention than ever before and speculation as to whether it could become an established and widely accepted way to pay for goods and services.

But Bitcoin isn’t the only cryptocurrency out there. Several others are also surging in popularity and value, and they claim to offer technical improvements that make them better suited to mainstream use.

Some of these competing currencies already represent significant stores of value. The value of a single bitcoin on the most popular exchange was $93.70 at time of publication, and the total value of all bitcoins in circulation just over $1 billion (it was over $2 billion at the market's high point last week). The largest alternative cryptocurrency, litecoins, were worth $2.31 each and $38 million in total; the next largest, PPCoin, were worth $0.22 each adding up to a total value of $4 million.

Bitcoin is based on mathematical techniques that control the production of new bitcoins, make it possible for a person to verify money sent to them is genuine, rule out counterfeiting, and limit the maximum number that can ever exist (to 21 million) (see “What Bitcoin Is, and Why It Matters” http://www.technologyreview.com/news/424091/what-bitcoin-is-and-why-it-matters/).

The Bitcoin alternatives are inspired by that design, which is published openly, and try to offer improvements.

One of Litecoin’s most significant claimed improvements over Bitcoin is that it allows transactions to be confirmed as legitimate much more quickly, says Charles Lee, who designed the currency, which is now maintained by him and a small group of other enthusiasts.

Read the rest here:
Tool reveals Apple user locations


An Australian researcher has created a tool that uses Apple’s location services to potentially reveal where users live.

The tool works by accessing Apple’s database of wireless access points, which is collected by iPhones and iPads that have GPS and WiFi location services enabled. Most iPhones and iPads regularly submit information about access points within range to Apple, regardless of whether users connect to them.

Apple uses this ‘crowd-sourced’ data to run its location services, however the location database is not meant to be public.

According to independent penetration tester Hubert Seiwert, Apple will reveal Mac address and GPS information on hundreds of nearby access points if a user queries the location of a single WiFi router's Mac address.

His proof-of-concept Python application, iSniff GPS, uses this process to allow users to view maps of nearby access points. “You can send Apple a single Mac address of a WiFi router and they will send back a result set including the GPS coordinates of that Mac address and about 400 others,” Seiwert said.

“You can plug that Mac address into Apple’s location service through iSniff GPS and you will get very precise information back from that.”

The tool makes use of a discovery last year by Immunity’s Mark Wuergler, who discovered that iPhones and iPads sometimes disclose sensitive information about previously joined access points when joining a new WiFi network.

If captured, this data could previously be used with Google’s location services to discover the locations of targeted devices.

Seiwert said Apple devices when joining networks will sometimes disclose via ARP requests the Mac addresses of the last three WiFi routers they have previously connected to, which will frequently include the device owner’s home WiFi router.

His tool captures these ARP requests along with multicast DNS and SSID name probes for previously joined networks.

“This could be used to locate where people live,” he said.

Read the rest here:

Digital Currency Operation Charged in $6 Billion Money Laundering Scheme

Mythili Raman, Acting Assistant Attorney General for the Criminal Division of the U.S. Department of Justice; Preet Bharara, U.S. Attorney for the Southern District of New York; Steven Hughes, Special Agent-in-Charge of the New York Office of the U.S. Secret Service; Richard Weber, Chief of the Internal Revenue Service, Criminal Investigation (IRS-CI); and James Hayes Jr., Special Agent-in-Charge of the New York Field Office of the U.S. Immigration and Customs Enforcement’s (ICE) Homeland Security Investigations (HSI), have announced the unsealing of an indictment charging Liberty Reserve, a company that operated one of the world’s most widely used digital currency services, and seven of its principals and employees with money laundering and operating an unlicensed money transmitting business. Liberty Reserve is alleged to have had more than one million users worldwide, including more than 200,000 users in the U.S., who conducted approximately 55 million transactions — virtually all of which were illegal — and laundered more than $6 billion in suspected proceeds of crimes including credit card fraud, identity theft, investment fraud, computer hacking, child pornography and narcotics trafficking.

Five defendants were arrested on May 24, 2013, including Arthur Budovsky, the principal founder of Liberty Reserve, who was arrested in Spain; Vladimir Kats, the co-founder of Liberty Reserve, who was arrested in Brooklyn, New York; Azzeddine El Amine, a manager of Liberty Reserve’s financial accounts, who was arrested in Spain; and Mark Marmilev and Maxim Chukharev, who helped design and maintain Liberty Reserve’s technological infrastructure, who were arrested in Brooklyn and Costa Rica, respectively. Two other defendants, Ahmed Yassine Abdelghani (Yassine) and Allan Esteban Hidalgo Jimenez (Hidalgo), are at large in Costa Rica.

In addition to the criminal charges brought in the indictment, five domain names were seized, namely, the domain name of Liberty Reserve and the domain names of four exchanger websites that were controlled by one or more of the defendants; 45 bank accounts were restrained or seized; and a civil action was filed against 35 exchanger websites seeking the forfeiture of the exchangers’ domain names because the websites were used to facilitate the Liberty Reserve money laundering conspiracy and constitute property involved in money laundering. The four exchangers whose domain names were seized, as well as the 35 exchangers whose domain names are the subjects of the civil forfeiture action, were all exchangers that transacted business with Liberty Reserve and were listed on Liberty Reserve’s website as “pre-approved exchangers.” The investigation and takedown involved law enforcement action in 17 countries, including Costa Rica, the Netherlands, Spain, Morocco, Sweden, Switzerland, Cyprus, Australia, China, Norway, Latvia, Luxembourg, the United Kingdom, Russia, Canada and the U.S.

Read the rest here:
Cyber attacks against FederalNewsRadio.com, WTOP.com part of growing trend

By Jason Miller, Federal News Radio, 5/13/2013

The cyber attacks suffered by FederalNewsRadio.com and WTOP.com last week are part of a growing trend of breaches that take advantage of network weaknesses to indiscriminately go after visitors of popular websites.

While some analysts attributed the recent cyber breach, which caused both media websites to turn off access via Internet Explorer from May 7-11, to a "watering hole" type of attack, all indicators point to it being a "drive-by" attack, said John Spaulding, Washington, D.C. director of information systems for Hubbard Radio, the parent company of WTOP and Federal News Radio.

Spaulding said a drive-by attack is one where the malicious code is hidden on a Web page and a computer gets infected by visiting the website. A watering hole attack, on the other hand, is where the hacker targets a specific group of people who tend to go to a specific site.

Spaulding said both FederalNewsRadio.com and WTOP.com have been scrubbed of malware and vulnerabilities have been plugged. Users of all Internet browsers could safely access both sites starting late Saturday night. He encouraged website visitors who accessed the websites from any Web browser during the cyber attack, which occurred approximately May 5 to May 7, to update and run their security software and perform a malware scan on their computer.

"The malware did not target an IE vulnerability. However, the way it was deployed favored IE as the browser it would use to infect computers," Spaulding said. "An intruder was able to exploit a different website hosted on our shared infrastructure. From there, they gained privileged access to WTOP.com and FederalNewsRadio.com after installing some hidden portals, which allowed them continued access to our sites. They implemented malicious code, which allowed malware to attempt to infect our site visitors' computers."

He added there is no evidence that indicates FederalNewsRadio.com and WTOP.com were specifically targeted.

Looking for money

Alma Cole, the former head of the Homeland Security Department's security operations center and now vice president of cybersecurity at Robbins Gioia, said a successful drive-by attack usually installs two distinct kinds of malware: Fake AntiVirus and a Zeus Bot Trojan.

"The presence of Fake AntiVirus software clearly indicates that this was cyber criminals looking to make money, not a Nation State (APT) interested in espionage," he said. "Zeus Bot is the most widespread criminal Trojan that is used primary for theft of banking and other credentials."

Cole added the attack does not resemble and is not related to the well publicized attacks against other news agencies, and would not have included an overt intrusion into the networks of Federal News Radio or WTOP. Some systems may have been infected but this would have been collateral damage, he said.


Symantec found in 2012, drive-by Web attacks increased by one-third, possibly driven by malvertising. Malvertising is an ad that is infected with malware so when a user clicks on it, their computer becomes contaminated.

"Drive-by infections from websites will become even more common and even harder to block without advanced security software," Symantec wrote in its report about what it sees as the future trends in cyber attacks. "Criminals will increasingly attack websites, using malvertising and website attack kits, as a means of infecting users. Software vendors will come under pressure to increase their efforts in fixing vulnerabilities promptly. Users and companies that employ them will need to be more proactive about maintaining their privacy and security in this new social media world."

Symantec said small businesses — those with less than 250 employees — were victims of 31 percent of all cyber attacks in 2012, up from 18 percent the year before.

"Driven by attack toolkits, in 2012 the number of Web-based attacks increased by one-third and many of these attacks originated from the compromised websites of small businesses," the report stated. "These massive attacks increase the risk of infection for all of us."

Johannes Ullrich, the dean of research and a faculty member of the SANS Technology Institute, said Web applications are much more complex today than ever before.

"They have a lot of parts they are composed of and it's really not easy to make sure all of them are secure," he said in an interview with Federal News Radio. "Probably the hardest task is to prove something is secure."

Read the rest here: http://www.federalnewsradio.com/?nid=241&sid=3320305
New Documents Suggest the IRS Reads Your Emails Without a Warrant

Nathan Freed Wessler, American Civil Liberties Union, April 11, 2013

Everyone knows the IRS is our nation’s tax collector, but it is also a law enforcement organization tasked with investigating criminal violations of the tax laws. New documents released to the ACLU under the Freedom of Information Act reveal that the IRS Criminal Tax Division has long taken the position that the IRS can read your emails without a warrant—a practice that one appeals court has said violates the Fourth Amendment (and we think most Americans would agree).

Last year, the ACLU sent a FOIA request to the IRS seeking records regarding whether it gets a warrant before reading people’s email, text messages and other private electronic communications. The IRS has now responded by sending us 247 pages of records describing the policies and practices of its criminal investigative arm when seeking the contents of emails and other electronic communications.

So does the IRS always get a warrant? Unfortunately, while the documents we have obtained do not answer this question point blank, they suggest otherwise. This question is too important for the IRS not to be completely forthright with the American public. The IRS should tell the public whether it always gets a warrant to access email and other private communications in the course of criminal investigations. And if the agency does not get a warrant, it should change its policy to always require one.

The IRS and Email: Reading Between the Lines

The federal law that governs law enforcement access to emails, the Electronic Communications Privacy Act (ECPA), is hopelessly outdated. It draws a distinction between email that is stored on an email provider’s server for 180 days or less, and email that is older or has been opened. The former requires a warrant; the latter does not. Luckily, the Fourth Amendment still protects against unreasonable searches by the government. Accordingly, in 2010 the Sixth Circuit Court of Appeals decided in United States v. Warshak that the government must obtain a probable cause warrant before compelling email providers to turn over messages.

However, the IRS hasn’t told the public whether it is following Warshak everywhere in the country, or only within the Sixth Circuit.

Let’s hope you never end up on the wrong end of an IRS criminal tax investigation.

The documents the ACLU obtained make clear that, before Warshak, it was the policy of the IRS to read people’s email without getting a warrant. Not only that, but the IRS believed that the Fourth Amendment did not apply to email at all. A 2009 “Search Warrant Handbook” from the IRS Criminal Tax Division’s Office of Chief Counsel baldly asserts that “the Fourth Amendment does not protect communications held in electronic storage, such as email messages stored on a server, because internet users do not have a reasonable expectation of privacy in such communications.”

Again in 2010, a presentation by the IRS Office of Chief Counsel asserts that the “4th Amendment Does Not Protect Emails Stored on Server” and there is “No Privacy Expectation” in those emails.

Other older documents corroborate that the IRS did not get warrants across the board. For example, the 2009 edition of the Internal Revenue Manual (the official compilation of IRS policies and procedures) explains that “the government may obtain the contents of electronic communication that has been in storage for more than 180 days” without a warrant.

Then came Warshak, decided on December 14, 2010. The key question our FOIA request seeks to answer is whether the IRS’s policy changed after Warshak, which should have put the agency on notice that the Fourth Amendment does in fact protect the contents of emails. The first indication of the IRS’s position, from an email exchange in mid-January 2011, does not bode well. In an email titled “US v. Warshak,” an employee of the IRS Criminal Investigation unit asks two lawyers in the IRS Criminal Tax Division whether Warshak will have any effect on the IRS’s work. A Special Counsel in the Criminal Tax Division replies: “I have not heard anything related to this opinion. We have always taken the position that a warrant is necessary when retrieving e-mails that are less than 180 days old.” But that’s just the ECPA standard. The real question is whether the IRS is obtaining warrants for emails more than 180 days old. Shortly after Warshak, apparently it still was not.

The IRS had an opportunity to officially reconsider its position when it issued edits to the Internal Revenue Manual in March 2011. But its policy stayed the same: the Manual explained that under ECPA, “Investigators can obtain everything in an account except for unopened e-mail or voice mail stored with a provider for 180 days or less using a [relevant-and-material-standard] court order” instead of a warrant. Again, no suggestion that the Fourth Amendment might require more.

Read the rest here:
How valuable are security certifications today?

By Lauren Gibbons Paul, CSOOnline, Apr 1, 2013

When it comes to education, most people agree, more is better. No one embodies that principle — at least in regard to IT certifications — better than Jerry Irvine, CIO of IT consulting firm Prescient Solutions and member of the National Cyber Security Task Force, Irvine holds more than 20 IT certifications, of which at least six are specifically information security-oriented.

"I'll stop getting certifications when I'm dead," says Irvine, though one wonders if even that will dissuade him. Irvine is a strong believer in the notion that the value of certifications in general and security certifications in particular shows up in your wallet.

"My opinion is the more certified you are, the more marketable you are. You can prove you know more because you have those certifications," says Irvine. "People look at you and say, 'This guy really does know his stuff.' That gives you the opportunity to make more money."

Anyone who puts in the time and spends the money to get certified is showing they care about staying current with security trends and techniques. That quality makes someone more desirable to an employer, he adds.

As a practical matter, many of today's information security certifications require much hands-on application of skills, such as CompTIA’s CASP (Certified Advanced Security Professional), which requires candidates to configure firewalls and routers and perform other security-related tasks as part of the test. Being able to pass proves to a potential employer that you can do certain things, potentially giving you an edge over those who do not hold the certification.

For some jobs, obtaining a particular security certification — whether for information security or physical security — is a requisite for even being considered. In that case, you will surely know if there is a certification you need to obtain. Beyond that, however, attaining certifications is generally a matter of personal and/or employer choice. Some certifications require a great deal of work both in and out of the classroom, as well as sitting for the test. The question: Do they generate return on your investment?

Certifications should not be the end goal so much as a tool you can use in furthering your career, cautions Chris Brenton, an instructor at the SANS Institute and director of information security for CloudPassage, a cloud security provider. Brenton has been delivering certification training for quite a few years but — perhaps surprisingly — does not hold any himself.

Read the rest here: http://www.csoonline.com/article/731010/how-valuable-are-

Rotten spam causing more infections than ever - study

By Neil McAllister, The Register, 11 April 2013

Anti-spam tools have evolved to a degree where many of us hardly see much spam anymore. But when we do, the threat posed by those messages is greater than it has ever been, according to a new report from independent security firm AV-Test.

The report, entitled "Spam – More Dangerous than Ever Before," was based on an 18-month study conducted between August 2011 and February 2013, in which AV-Test harvested and analyzed some 550,000 spam emails.

As in the past, the vast majority of those messages contained fraudulent offers for counterfeit products, such as bogus pharmaceuticals. Being ripped off is the main risk there, not to mention phishing.

But around 2.5 per cent of the spam being sent today serves a different, darker purpose, the report claims – namely, spreading malware.

Certain types of spam emails are especially dangerous. Of the 30,000 spam messages AV-Test analyzed that contained attachments, over 10,000 of them – nearly a third – were infected with malware.

The file formats used to deliver the payloads were mostly the usual suspects. ZIP attachments and executable formats such as EXE and PIF were almost always infected, as were 80 per cent of HTML documents sent as attachments. PDF and image attachments were occasionally found to contain exploits, too.

Less prevalent, but much harder to spot, were messages containing links to websites that spread malware. Only around 1 per cent of the spam that included URLs contained such links, but such messages are often indistinguishable from those containing more benign links.

But not all spam is created equal. In particular, country of origin matters when determining whether a message is likely to contain malware.

As with other studies, AV-Test found that the majority of all spam sent originates in the United States, including spam messages containing attachments. But only 15 per cent of spam attachments sent from the US were actually malware, compared to 30 per cent globally.

Read the rest here: http://www.theregister.co.uk/2013/04/11/spam_more_dangerous_than_ever/
I'm a Fortune 500 Company and I've Been Hacked

Symantec report finds small businesses battered by cybercrime

By Mark Hatton, SecurityWeek, April 09, 2013

One of the more interesting cyber security phenomena I've witnessed recently is not only the willingness of CEOs to admit that their company has suffered a breach, but the enthusiasm in which they have shown in making the admission.

In what seems like only a short-time ago, company management, often on the advice of legal counsel, had no appetite to discuss issues of cyber security. This was especially the case when it had been compromised. Yet here we are today and the leaders of some of the world’s best-known brands are “raising their hands” and talking openly about the subject. So what changed?

I believe the change in attitude is the result of external pressure from two separate, and potentially competing, sources. First, the Securities and Exchange Commission (SEC) has been encouraging greater transparency from public companies to disclose breaches, even if they don’t involve a material incident. By law, companies must disclose breaches that affect shareholder value. According to the National Conference of State Legislatures (NCSL), 46 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving customers’ personal information.

The threat of potential non-compliance with government standards has been a driving force in changing corporate policies on not only what should be disclosed in terms of a breach, but also when and how it should be disclosed. While negative public perception has always been a primary reason to remain quiet, when balanced against the threat of state and federal action, it becomes the lesser of two evils in the eyes of most board members and executives.

The second factor I see influencing the decision to “go public” as the victim of a breach is that trendsetting entities such as Apple, Google and Facebook have made it ok to do so. Once these companies, viewed as the leaders in Internet technology, came out and essentially said, “We’ve been hacked, this is how they did it, and this is what they were after,” it has in many ways become almost the fashionable thing to do, or at least less embarrassing.

Read the rest here:

By Jeremy Kirk, IDG News Service, 16 April, 2013

Cybercriminals are increasingly targeting small businesses due to their less sophisticated defenses, according to a new report from Symantec.

Companies with 250 employees or less absorbed 18 percent of targeted cyberattacks in 2011, but the figure jumped to 31 percent in 2012, Symantec said in its Internet Security Threat Report 2013, released on Tuesday.

"While it can be argued that the rewards of attacking a small business are less than what can be gained from a large enterprise, this is more than compensated by the fact that many small companies are typically less careful in their cyberdefenses," the report said.

Organizations between 251 employees to 2,500 were targeted 19 percent of the time, with companies with more than 2,500 employees making up the remaining 50 percent, Symantec said. The company said it detected a 42 percent increase overall in cyberattacks in 2012 compared to 2011.

Employees in research and development and sales functions are prime targets for hackers, and Symantec said it saw a large increase in attacks directed at those roles. "This suggests that attackers are casting a wider net and targeting less senior positions below the executive level in order to gain access to companies," the report said.

The websites of small businesses also prove attractive to criminals to plant malicious software in order to gain a foothold in other companies. If a user visits a hacked website, the person’s web browser will be probed for software vulnerabilities. The method of using a company’s website as bait is termed a “watering hole” attack by Symantec.

"For example, an attacker may infiltrate a small supplier in order to use it as a spring board into a larger company," Symantec wrote.

Small businesses may have less cash on hand for hackers to steal, but the companies may have other data, such as customer information or intellectual property, that is valued by hackers.

Read the rest here:
How video analytics helps reconstruct Boston Marathon bombings


Video from surveillance cameras and people’s cell phones are increasingly valuable resources in helping investigators collect and analyze data from crime scenes, such as the finish line of the Boston Marathon. Investigators are combing through hours of digital feeds and thousands of photographs to identify suspects responsible for detonating two bombs there on April 15.

On Thursday morning, authorities were reportedly set to release photos of two suspects in the bombings, although the analysis of all that footage will undoubtedly continue, as the police and FBI seeks to piece together the chain of events. (UPDATE: The FBI released photos of the suspects Thursday night, asking for help in identifying them. Later, one of the suspects, identified as brothers, was killed in a confrontation with police that also left a security officer dead, and the second suspect was still being sought.)

But how do investigators weed through terabytes of video in different formats, whether 30-second snippets from cell phones or hours of footage from a surveillance camera at a nearby store? Going through all that footage is still largely a labor-intensive task, but video analytics and digital forensics tools can help investigators compress video, pinpoint areas of interest, look for anomalies and find relevant details, according to government and industry experts.

Many video surveillance systems come packaged with analytics that can detect anomalies, such as a package left behind or a person entering a restricted area, said Maj. David Mulholland, commander of technical services with the United States Park Police. Because humans can’t watch multiple security feeds without being overwhelmed or losing attention, analytics software signals -- visually or through audio -- if someone enters a stairway where no person should be, he said.

There are also video analytics tools that compress long hours of video. Video Synopsis, a tool for CCTV surveillance systems from Briefcam, an Israel-based company with offices in Connecticut, lets investigators pinpoint an area of interest and show only the moments where something was different in that picture. Admittedly, that would be more challenging in a race, where something is changing every second than, say, at an office overnight where someone might take a folder off a desk, make copies and return the folder, Mulholland said. But instead of watching eight hours of video, investigators can compress the footage down to the three-minute period in which the folder was taken from the desk. That’s a start, a baseline, he said.

“The next thing you can do with the analytic capability is identify an area of interest within the camera frame,” Mulholland said. For example, once investigators have identified the origin of a detonation of a bomb, they can draw an area of interest. There may have been 500 people who walked in that general area, but the analytics piece will ignore that and flag anything that changed in that one specific area—such as a backpack being left behind. So instead of spending 20 minutes looking at video in which nothing happens, the investigator can hit a button and in 30 seconds go to the area of interest and then begin to dissect what actually happened, Mulholland noted.

There are different flavors of this software out on the market. BRS Labs’ AiSight, a behavioral analysis system for video surveillance, adaptively “learns” behavior patterns in complex environments. The video surveillance software uses a reason-based approach versus legacy rules-based technology, company officials say. Because humans are not required to define the rules for object or behavior recognition, the system can easily scale to thousands of cameras.

But the ability to define parameters is a critical feature for video analytics software, Mulholland said. For example, there might be a gateway into the viewing area of a venue that people are only supposed to exit through — so someone entering through the exit could be of interest. You would want to define a parameter saying, “show me if someone is going against the normal flow of pedestrian traffic.” Or if investigators know a suspect was wearing a red shirt, they could put that into the parameters and say, “show me someone who is wearing a red shirt.”

Data and time-based review video submitted by ordinary citizens and the use of various image and pattern recognition software might also help identify potential suspects in the bombing, according to Lee Neubecker, president of Forensicon, a developer of digital forensic tools.

Neubecker demonstrated how he analyzed video of one of the bomb blasts that was submitted to Boston.com. By slowing the video down and colorizing it, he was able to show debris from the explosion hurling through a window of a nearby building, which could point investigators to debris from the pressure cooker bomb. Then investigators could determine where the pressure cooker was manufactured and analyze sales receipts from local retailers. Using facial recognition software and video forensics, they then could cross reference security video of people buying pressure cookers with images — such as those of the two suspects — taken at the marathon finish line, Neubecker said.

Read the rest here: http://gcn.com/Articles/2013/04/18/How-video-analytics-reconstruct-Boston-Marathon-bombings.aspx?Page=1
Preventing Misinformation from Spreading Through Social Media

New platforms for fact-checking and reputation scoring aim to better channel social media’s power in the wake of a disaster.

By David Talbot, MIT Technology Review, April 23, 2013

The online crowds weren’t always wise following the Boston Marathon bombings. For example, the online community Reddit and some Twitter users were criticized for pillorying an innocent student as a possible terrorist suspect. But some emerging technologies might be able to help knock down false reports and wring the truth from the fog of social media during crises.

Researchers from the Masdar Institute of Technology and the Qatar Computing Research Institute plan to launch Verily, a platform that aims to verify social media information, in a beta version this summer. Verily aims to enlist people in collecting and analyzing evidence to confirm or debunk reports. As an incentive, it will award reputation points—or dings—to its contributors.

Verily will join services like Storyful that use various manual and technical means to fact-check viral information, and apps such as Swift River that, among other things, let people set up filters on social media to provide more weight to trusted users in the torrent of posts following major events.

On Reddit, amateur sleuthing to identify possible bombing suspects led to accusations against a student, Sunil Tripathi, a Brown University student reported missing weeks earlier (an apology has since been issued by Reddit); that accusation was then tweeted and retweeted many times. “The underlying problem is a fearsome one—people want to share and spread information, whether accurate or not,” says Ethan Zuckerman, who directs the center for civic media at MIT. “We’re very far from a solution. The reporting around the Marathon bombing demonstrates that mainstream media has issues with verification that are as profound as anything we face online.”

Reputation scoring has worked well for e-commerce sites like eBay and Amazon and could help to clean up social media reports in some situations.

Research efforts have also shown how to effectively mobilize many people on social media for a common task. In a 2009 experiment, the U.S. Defense Advanced Research Projects Agency offered $40,000 to the first team that could identify the locations of 10 large red weather balloons lofted by DARPA at undisclosed locations across the United States. The winning team, from MIT, did it in less than nine hours using an incentive structure, fueled by cash rewards, to drum up viral participation on social media. Anyone who found a single balloon would get $2,000; someone who invited that person to join the hunt would get $1,000. A similar but harder challenge, in 2012, asked teams to find specific individuals within cities within 12 hours with only a single mugshot to work with. There again, a distributed cash reward system worked best.

Verily builds on lessons from both contests. The winning mugshot team included one of Verily’s creators, computer scientist Iyad Rahwan, a graduate of MIT who is now at the Masdar Institute of Technology. “Recruiting people to join is part of the issue, but we also need to figure out how to remove false reports,” Rahwan says. “Where the balloon challenge took nine hours, we hope to facilitate the crowdsourced evaluation of multimedia evidence on individual incidents in less than nine minutes.”

The beta version of Verily will first be tested by its creators on a real-world weather disaster such as a hurricane or flood. Since such disasters come with some warning, Verily’s creators can prepare humanitarian agencies to use the platform. A piece of reported news—such as a photo of a flooded hospital circulating on Twitter—would be posted to Verily with a question: is the hospital really flooded? Users would then examine the photo for signs of authenticity and also leverage their own social networks to investigate its authenticity.

Humanitarian agencies working in the region could promote participation, as could the press and Twitter. Voters’ reputation scores would increase or decrease over time; future votes from reliable people would get increased weight. And voters would be encouraged to bring others to the site; anyone brought in by someone with a good reputation would automatically start with a higher reputation themselves.

Read the rest here:
The U.S. Department of Defense has revealed that it is now spending $30 million to set up offensive Cyber War operations in the army and air force. Two-thirds of the money is being spent by the air force which has traditionally taken the lead in Cyber War matters. The money is being spent mainly to buy hardware for the hackers, as well as software tools.

Offensive Cyber War involves a lot more than just trying to hack your way into specific enemy computers and networks. First you have to find out what you are up against. This begins with mapping where everything on enemy networks is. China was noted doing this back in 2005 and the mapping they were doing was a prerequisite to a major attack on non-Chinese systems that is still underway.

After the initial mapping you select the best targets. This is done by determining which systems yield the best impact (which ones have the most valuable information and/or are the most vulnerable). Then you go in and collect more information on specific attacks on military targets. After that you carry out the attacks.

The mapping is part of a military operation and the Chinese know that. You have to assume they will respond to the mapping, which is why the mapping is a constant process. Mapping is also done by professional Internet criminals in preparation for their more mercenary attacks (Internet fraud). Over the last decade Internet fraud has been largely taken over by highly disciplined gangs, rather than lots of individual hackers. The gangs are well organized, and have the resources to carry out extensive mapping operations. Thus many periods of heavy mapping activity is usually a prelude to major Internet based heists. Even government and military sites are valuable targets for the Internet hacking gangs, because valuable information can be sold on the black market. Governments have been known to hire the gangs for specific jobs, or simply let it be known on the black market (for data stolen by hackers) that certain types of data held by some governments will fetch a particularly high price.

The most valuable information in Cyber War offensive operations is data from enemy hackers. Stealing their tools and data (especially mapping and target selection data) is the most valuable prize of all. A lot of it is kept off line to prevent that, but one function of mapping is to discover where someone may have screwed up and left some valuable information available via the Internet.

Read the rest here:
http://www.strategypage.com/htmw/htiw/articles/201304
In current threat landscape, cyber teams need to go looking for trouble

By William Jackson, GCN, May 17, 2013

Agency cybersecurity teams have not been accepted by IT shops as full partners in the job of supporting agency missions and as a result are falling farther behind in efforts to detect and block threats, said security analyst Mischel Kwon.

“That’s our fault,” said Kwon, president of Mischel Kwon and Associates and a former government cybersecurity official.

Security needs to adopt a more aggressive posture, seeking out threats rather than just detecting them and working with IT departments to follow through on remediation. Breaking down the walls between security and IT could enable better risk management and risk mitigation, Kwon said in a presentation at the FOSE conference in Washington, D.C. Keeping threat detection and mission support functions in separate shops hampers security in the face of increasingly complex attacks, she said.

Cyber threats have evolved in recent years, with familiar exploits and tools being used in compound attacks that are becoming more effective in slipping through defenses.

These malicious tools also are being used in new ways, with hacktivists indulging in espionage and sabotage alongside nation-states and criminal groups. Denial of service attacks are seeing a resurgence in popularity and effectiveness, and the Defense Department has publicly identified China as a source of cyber intrusions against U.S. private and public-sector assets.

These changes have raised both the profile and the stakes of cybersecurity, Kwon said. “Maybe it’s time we looked at it differently,” she said of the threat landscape.

Security needs to take a broader view of detection, doing more packet and traffic analysis to discover patterns and identify threats before they are inside the systems and follow through on the remediation of weaknesses that are being targeted.

Read the rest here:
http://gcn.com/articles/2013/05/17/cyber-teams-need-to-look-for-trouble.aspx

Should we be worried about cyberterrorism? Without a doubt

By Frank Miele, Daily Inter Lake, May 18, 2013

On Monday May 6, I stumbled across an Internet news story in the Washington Times about a threatened cyberterror attack that was scheduled to occur on Tuesday, May 7.

According to this story by Shaun Waterman (http://www.washingtontimes.com/news/2013/may/6/jihadis-and-hackers-teaming-launch-cyberattacks-us/), the Department of Homeland Security had sent a bulletin to “the private sector” (probably banks and major corporations) about the threatened attack against high-profile targets such as government agencies and financial institutions.

The source for the Washington Times story was Brian Krebs, former Washington Post reporter, who now blogs at KrebsOnSecurity.com where he writes about Internet security.

On May 2, Krebs had written about a May 1 confidential alert by Homeland Security predicting that the May 7 attack would “mostly consist of nuisance-level attacks against publicly accessible webpages and possible data exploitation. Krebs posted the original anonymous threat, which was posted on April 21, as well as a PDF of the Homeland Security document warning about “efforts by mostly Middle East- and North Africa-based criminal hackers and cyber actors to plan and launch cyber attacks aimed at US Government agencies, financial institutions, and commercial organizations in a campaign known as ‘OpUSA’.”

Fortunately or unfortunately, I am not a bank, a major corporation or a government agency, so although I found the story interesting, I promptly put it out of my mind — at least until I woke up the following morning, May 7, and discovered that my Internet service was down at my home.

I called CenturyLink’s hotline and discovered that they knew about the problem and expected it to be resolved within 24 to 48 hours. Then I went to work and discovered that the Internet service was down there, too. Within an hour or two, I had learned (using my cell phone) that CenturyLink Internet service was down pretty much nationwide, affecting at least 1 million residential and business Internet consumers.

Read the rest here:
http://www.dailyinterlake.com/opinion/columns/frank/article_95f7dcede-bf68-11e2-8e53-001a4bcf887a.html
Chinese Hackers Resume Attacks on U.S. Targets

By David E. Sanger and Nicole Perlroth, NY Times, May 19, 2013

Three months after hackers working for a cyberunit of China’s People’s Liberation Army went silent amid evidence that they had stolen data from scores of American companies and government agencies, they appear to have resumed their attacks using different techniques, according to computer industry security experts and American officials.

The Obama administration had bet that “naming and shaming” the groups, first in industry reports and then in the Pentagon’s own detailed survey of Chinese military capabilities, might prompt China’s new leadership to crack down on the military’s highly organized team of hackers — or at least urge them to become more subtle.

But Unit 61398, whose well-guarded 12-story white headquarters on the edges of Shanghai became the symbol of Chinese cyberpower, is back in business, according to American officials and security companies.

It is not clear precisely who has been affected by the latest attacks. Mandiant, a private security company that helps companies and government agencies defend themselves from hackers, said the attacks had resumed but would not identify the targets, citing agreements with its clients. But it did say the victims were many of the same ones the unit had attacked before.

The hackers were behind scores of thefts of intellectual property and government documents over the past five years, according to a report by Mandiant in February that was confirmed by American officials. They have stolen product blueprints, manufacturing plans, clinical trial results, pricing documents, negotiation strategies and other proprietary information from more than 100 of Mandiant’s clients, predominantly in the United States.

According to security experts, the cyberunit was responsible for a 2009 attack on the Coca-Cola Company that coincided with its failed attempt to acquire the China Huiyuan Juice Group. In 2011, it attacked RSA, a maker of data security products used by American government agencies and defense contractors, and used the information it collected from that attack to break into the computer systems of Lockheed Martin, the aerospace contractor.

More recently, security experts said, the group took aim at companies with access to the nation’s power grid. Last September, it broke into the Canadian arm of Telvent, now Schneider Electric, which keeps detailed blueprints on more than half the oil and gas pipelines in North America.

Representatives of Coca-Cola and Schneider Electric did not return requests for comment on Sunday. A Lockheed Martin spokesman said the company declined to comment.

In interviews, Obama administration officials said they were not surprised by the resumption of the hacking activity. One senior official said Friday that “this is something we are going to have to come back at time and again with the Chinese leadership,” who, he said, “have to be convinced there is a real cost to this kind of activity.”

Mandiant said that the Chinese hackers had stopped their attacks after they were exposed in February and removed their spying tools from the organizations they had infiltrated. But over the past two months, they have gradually begun attacking the same victims from new servers and have reinserted many of the tools that enable them to seek out data without detection. They are now operating at 60 percent to 70 percent of the level they were working at before, according to a study by Mandiant requested by The New York Times.

The Times hired Mandiant to investigate an attack that originated in China on its news operations last fall. Mandiant is not currently working for The New York Times Company.

Read the rest here:
http://www.nytimes.com/2013/05/20/world/asia/chinese-hackers-resume-attacks-on-us-targets.html?pagewanted=all&_r=1&
Article for the Newsletter?
If you would like to submit an article...

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:
doncream-issa@q.com

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

采用注入病毒删除数据等措施瘫痪敌计算机网络

Use virus insertion, deletion of data, and other techniques to paralyze enemy computer networks.
Volunteers Needed

Deborah Johnson is soliciting volunteers for the next ISSA-COS conference committee. Please contact her if you have an interest in helping on this committee.

The first task at hand is to choose a venue. We need to find a location with the following characteristics:

- Seats up to 200 people
- Good Visibility for all participants
- Adequate Parking
- Catering / Can we bring our own?
- Catering / Costs
- Audio / Visual equipment if available
- Other miscellaneous

If you are interested in helping on this committee, please contact her (djohnson@swcp.com). We can schedule some field trips to take a look at the venues and sample the menu, so to speak. Here are some possibilities: http://www.cvent.com/rfp/colorado-springs-co-event-venues.aspx

There are other planning tasks that need to be handled as well, such as marketing and publicity, brochures, programs, sponsors, door prizes, etc. so if you would like to take on any of these roles, let me know.

Thank you in advance!

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 13</td>
<td>11:00 to 1:00</td>
<td>Bambino's Italian Eatery and Sports Bar, 2849 East Platte Avenue, Colorado Springs, 719) 630-8121</td>
</tr>
<tr>
<td>Jul 11</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Aug 8</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Sep 12</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Oct 10</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Nov 14</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Dec 6</td>
<td>11:00 to 1:00</td>
<td>Carrabba’s North</td>
</tr>
</tbody>
</table>
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.

If your brain were a computer, how much storage space would it have?

By Robert T Gonzalez, io9, May 24, 2013

The comparison between the human brain and a computer is not a perfect one, but it does lend itself to some interesting lines of inquiry. For instance: what is the storage capacity of your brain?

The answer to the first question – how much storage space is there inside the average human head? – varies considerably, depending on who you ask. Some estimates come in as low as 1 terabyte, or approximately 1,000 gigabytes. These days, you can purchase an external hard drive with twice that capacity for under a hundred bucks.

Read the rest here:
http://io9.com/if-your-brain-were-a-computer-how-much-storage-space-w-509687776

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