It’s December Already!

Colleagues,

I can’t believe it is December already. It’s been a busy year for our chapter and I’m excited about what we as a chapter have accomplished and where we are headed in 2015. One of my biggest “cares” is how do we as a chapter continue to meet your needs while keeping things interesting. It’s very easy to fall into the rut of doing the same thing over and over, and I don’t want us to be a chapter that does that. We need to stay active, continually challenge the status quo, and ensure the energy in our chapter stays up.

We’re making small changes like having the speaker talk right after food is served for 45 mins with another 15 mins reserved for Q&A. This will help ensure our meetings provide a solid educational opportunity. The other part of that is ensuring we continue to work hard to get speakers that will inform us, challenge us, educate us, etc. We’re doing that by reaching out to many different corporations, businesses, and individuals because we want speakers with different backgrounds and experiences. If you know of any speakers you would like to hear from or specific topics you would like briefed please let me know. Once the speaker portion is over we will have a meeting that generally lasts no more than 30 minutes. I think now that we have our by-laws set keeping the meeting portion down to 30 minutes should be no problem.

We’re going to continue to put on three conferences a year and need your ideas and help on those. This year our summer conference will be called the Cybersecurity Training and Technology Forum and the first day we’re probably going to tie a job fair in with it which should provide our members with another opportunity if they need it and greatly help with the conference attendance as well. We’re still in the early planning stages of this, but we are working with our friends at the Federal Business Council to plan this event once again. We are excited about the changes going on.

(Continued on page 3)

The ISSA Colorado Springs Newsletter incorporates open source news articles as a training method to educate readers on security matters in compliance with USC Title 17, Section 107, Paragraph a.

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.
Anonymous statement: KKK is a terrorist group, KKK responds poorly

By Violet Blue, ZDNet, November 18, 2014

The Ku Klux Klan (KKK) threatened to use lethal force against Ferguson protesters; Anonymous successfully retaliated against the Ku Klux Klan's Ferguson threats by taking over two primary Twitter accounts, keeping KKK websites offline and outing KKK members.

In its statement on Monday night, Anonymous explained that through the Klan's Twitter account, it obtained large amounts of information on multiple white supremacists, and "members of Anonymous who seized the account are continuing to debate if the identities of the people associated with the Klan's account should be released to the public."

"We want to be sure we are ousting the right people. It would be against everything Anonymous does if we publicly released the information of the innocent..." "Once the operation is considered a complete success, we will remove the account from Twitter."

"What we accomplished 16 Nov 2014 is just the beginning..."

Last week, a Ku Klux Klan group based 75 miles south of Ferguson, Missouri, began distributing flyers threatening "lethal force" against Ferguson protesters in any aftermath of the upcoming grand jury decision regarding Ferguson police officer Darren Wilson.

The Missouri group behind the threats — Traditionalist American Knights of the Ku Klux Klan — is listed as an active hate group by the Southern Poverty Law Center.

The Ku Klux Klan responded poorly

Anonymous responded by first skirmishing with the KKK on Twitter, then declaring cyberwar on the racist group — with the Ku Klux Klan threatening Anonymous.

The KKK's "ace hacker" apparently decided to take some time off.

On Monday, Imperial Wizard Frank Ancona, who heads the Traditionalist American Knights of the KKK, told the Daily News, "Sounds to me like a bunch of kids in their mom's basement whacking off."

On Sunday, Anonymous exposed Ancona as a police officer who attended a Darren Wilson rally.

The KKK's response is in line with the racial segregation group's ongoing reaction to being pwned by Anonymous repeatedly over the past few days.

After the Klan's Twitter account @KuKluxKlanUSA mocked and threatened Anonymous, it was then seized by Anonymous, giving the hacktivist entity control of the KKK's largest public Twitter account.

That same day, the Klan set up a second account, @YourKKKcentral, where it issued threats "to call the FBI!" Anonymous quickly took control of that account, as well.

Since the takeover of both primary KKK Twitter accounts, Anonymous has been unrelenting in its focused attacks on the hate group's online presence. No one is surprised that the KKK is bad at both computer security and opsec.

Anonymous has kept the pressure on KKK websites ikkkk.com and TraditionalistAmericanKnights.com, both of which have been unable to resolve for at least 20 hours. The "Traditionalist Knights" website is apparently a CloudFlare customer, and the distributed denial-of-service (DDoS) protection service is noticeably struggling under the assault.

The KKK's website for its largest message board, Stormfront, has been knocked offline repeatedly, coming back with a plea from the KKK members who run it to donate help and money toward the site's security.

Read the rest here:
http://www.zdnet.com/anonymous-statement-kkk-is-a-terrorist-group-kkk-responds-poorly-700035890/
First, I'd like to welcome those new members on behalf of the Chapter! When you’re participating in Chapter activities, please take a moment to introduce yourself to members of the board, me, and other members. Don’t forget to identify yourself as a new member and feel free to ask for help or information.

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 will continue to sponsor student memberships so if you are interested, please contact me to coordinate the details. Each membership costs $55 per year including chapter dues. I’ll be happy to work with you if you have special requests such as male/female, veteran, etc. Contact me if you’re interested in becoming a sponsor. Also, if you know a specific student at any of the local universities you’d like to sponsor, I can work with you on that too.

We have good news about our 2014 membership drive so far. We’ve added a total of 99 new members this year. So, everyone, give yourselves a huge pat on the back and continue to bring in new members. Keep recruiting as we extend our goals for the year. Also, don’t forget to remind your peers and friends to renew, too. We’ve still got some work to do to get to our goal of 400 members but we are getting closer. Let’s get there by the end of the year!

As a separate activity, we have been working to establish a student mentorship program. Melissa has linked all the students with mentors and we’ll start having individual meetings beginning in December. We’ll be rotating mentors and students so everyone will get opportunities with multiple people. This variety should maximize student exposure to several mentors so everyone gets as much as possible from the effort. It should also help us develop the program going forward. All new students interested in being part of the mentoring program should contact Melissa or Dave. The student mentoring program now has a solid base of mentors, but we can definitely use more. Thank you to all who have volunteered already. Melissa Absher is the chairperson of the Student Mentorship Committee. Please see Dave or Melissa if you are interested in being a mentor.

Thanks for all your efforts and support.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

A Note From Our President

(Continued from page 1)

Again, please help us keep your chapter engaged on issues that make you more effective in your cybersecurity role…or whatever your specific job is. Your Chapter Board of Directors wants to ensure we meet your needs so send your ideas to us, talk to us at meetings, and let’s keep our chapter focused on the right areas as we move forward together.

Have a great holiday season and thanks for your support of the Colorado Springs ISSA.

Merry Christmas and Happy New Year.

Pat
Cybersecurity for the holidays:
A non-stop job

By Elizabeth Weise, USA Today, November 25, 2014

The holiday sales season and the online crush that accompanies it might seem a natural field day for hackers looking to attack the small and midsize retailers who depend on these sales to bump them into the black.

Surprisingly, it's not.

An analysis by IBM finds that cyberattacks don't peak during November and December. That's good, because security and IT staff are slammed as they are just making sure nothing breaks during the crucial sales season.

The list of things that could go wrong for retailers is far too long for comfort, security experts say. While many businesses see a downturn in activity over the holidays, for retail it's their lifeblood.

They know their employees could fall prey to "phishing" e-mails enticing them to disclose account information. They could unknowingly download malicious software by surfing the Web. Or they could use easy-to-break passwords.

Seasonal temp workers represent a huge potential weakness to the best-designed systems, said Akili Adjaoute, CEO of Brighterion, a San Francisco-based security firm.

"These less-trained workers that are hired during the holiday season are much more vulnerable to social engineering attacks," he said.

Training and actual bans on accessing the Web are key to avoiding trouble, according to a report by the Retail Cyber Intelligence Sharing Center.

Otherwise, "During low-volume hours, cashiers, clerks and seasonal workers may find fun things to do on the Web," the center said in a report issued this month.

Anything that could knock out a company's ability to sell online represents a huge blow to profitability. This year, Black Friday online sales are projected to be $2.48 billion, according to Adobe Systems' Digital Index online shopping forecast. Cyber Monday is projected to have sales of $2.6 billion.

IBM's Managed Security Service analyzed several years' worth of data loss records at USA TODAY's request and found that the Thanksgiving holiday weekend is not when crooks come calling.

"I went into this thinking it seems likely that corporations are attacked more during Black Friday — it's ripe for attack," said John Kuhn, an IBM senior threat researcher.

But when he looked, Kuhn couldn't find an uptick in attacks during the holidays, "not just to the retail industry, but for any industry," he said.

He speculates that attacks occur all year, as hackers are constantly looking for systems to infiltrate. Once in, they often spend months collecting and sneaking out data.

That's good news but no reason for companies to let down their guard. Hackers may not strike in December, but if they got there during swimsuit season, Christmas sales will suffer.

Protecting, testing and guarding systems to ensure there are no infiltrations and that the company's payment system can withstand denial-of-service and other brute-force attacks is crucial, say experts.

"It takes roughly six months to really prepare" for the holiday season online, said Peter Tran of computer security firm RSA.

Read the rest here:
Professional Ethics in the Digital Forensics Discipline

By Sean Harrington, DFINews, March 4, 2014

Mere days after a government crackdown on a spyware manufacturer comes the startling revelation that law enforcement agencies have been purchasing commercial spyware themselves and handing it out to the public for free.

Digital forensics examiners all confront ethical dilemmas made possible because they use privileged access to information systems and data, and because their services are almost always engaged incident to controversies. Examiners at one time or another will be exposed to trade secrets, threats to national security, information that private parties may pay handsomely for (or for the spoliation thereof), and highly personal information, including diaries, notes, personal photographs, and the like. Evidence found, overlooked, or determined not to exist by an examiner may decide the outcome of a multi-million dollar case, whether someone is imprisoned or set free, or which parent will be awarded custody of a child.

In fact, examiners are ill prepared to solve these dilemmas. The reasons include the lack of industry regulation, a paucity of ethics coverage in training curricula, and that the law applied to this subject matter is not well settled.1 Arguably, what is needed in the digital forensics profession is some combination of “good moral character,”2 an above-average understanding of evolving law, a well-drafted engagement contract, and continuing ethics training. Such a combination might equip the examiner either with the ability to answer some of the questions, or at least to spot the dilemma, so that he or she can seek advice from a mentor or legal counsel.

The profession has, for its part, endeavored to provide examiners with a framework within which the digital forensics examiner must not only recognize, classify, and manage ethical dilemmas, but also respect boundaries and honor obligations. This framework is the code of ethics, and this comment is intended to examine the need for and contours of these codes.

The Need for Professional Ethics in Digital Forensics

The relatively recent and rapid evolution of computers and information systems has resulted in novel capabilities to store, retrieve, and process information. In just the few years preceding this writing, new fields of expertise, such as “ethical hacking” and cloud forensics3 have emerged, all of which have added to the “huge demand” for highly educated specialists in the discipline of digital forensics.4 Likewise, the capabilities made possible by the evolution of computers and information systems have given rise to novel controversies regarding boundaries and obligations, intellectual property rights, privacy rights, diplomatic relations and military affairs, critical infrastructure, and the public welfare. Although some controversies can (and should) be anticipated and prospectively addressed by contract, the remainder, whether novel or familiar, are to be resolved in civilized societies by the courts of law.5 But both civil and criminal law has failed to keep pace with technological and societal trends catalyzed by technological advances.6 For example, neither statutory language of the Electronic Communications Privacy Act nor its legislative history makes any reference to the Internet.7 And even where the law may seem certain, pursuing a judicial remedy is costly and burdensome. Consequently, certifying organizations have adopted a code of professional ethics to provide examiners with the framework necessary to avoid or mitigate liabilities likely to require judicial remedies or likely to bring disrepute to the organization.8 In this regard, the code of ethics provides articulable principles against which one’s decision-making is objectively measured. Codes of ethics serve other important interests, including presenting an image of prestige and credibility for the organization and the profession,9 eliminating unfair competition,10 and fostering cooperation among professionals.

One way to define codes of ethics may be to suggest what the code of ethics is not: first and foremost, it should not be regarded as mere aspirational platitudes. And, it is neither an approximation of nor a substitute for the law. Rather, the code of ethics is designed to establish a minimum standard of acceptable conduct for all reasonably foreseeable activities within the profession. Such activities include: representations of one’s skills and expertise; research; interactions with clients, supervisors, government authorities, judicial officers, and attorneys; collection, preservation, and analysis of evidence; testing (i.e., validation of hardware and software tools); consultation (advising); report writing; testifying; mentoring; teaching; and continuing education. Further, as discussed above, cyber forensics involves recognizing, classifying, and managing ethical dilemmas, respecting boundaries, and honoring obligations. In light of the wide range of cyber forensics activities, one other thing to say the code is not is an exhaustive list of prohibited behaviors or of permissible behaviors.

Read the rest here:
http://www.dfinews.com/articles/2014/03/professional-ethics-digital-forensics-discipline-part-1
Cyber Security: Your Mother Was Right, Sharing is Good, And NIST Has Some Help on How

By NIST Tech Beat, November 10, 2014

Time is not your friend when your information systems are under cyber attack, but sharing threat information before, during, and after an attack with a trusted group of peers can help. Not only does it alert the other members of your community to a potential attack, it can provide critical actionable information to speed and bolster your own defenses. Participating in a formal information sharing group can greatly enhance an organization’s cybersecurity capabilities.

But for all the potential benefits, sharing operational information outside an organization presents a unique set of challenges. To help, the National Institute of Standards and Technology (NIST) has prepared a Guide to Cyber Threat Information Sharing (http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-150) that provides organizations with the key practices they need to consider when planning, implementing and maintaining information sharing relationships. NIST is requesting comments on the draft document by November 28, 2014.

An organization that has faced an attack has valuable information to share with others. “By sharing cyber threat information, organizations can gain valuable insights about their adversaries,” says lead author Christopher Johnson. “They can learn the types of systems and information being targeted, the techniques used to gain access and indicators of compromise. Organizations can use this information to prioritize defensive strategies including patching vulnerabilities, implementing configuration changes and enhancing monitoring capabilities.”

Information sharing within business sectors is particularly advantageous because the organizations often face similar threats.

The NIST publication presents a deeper treatment of the information-sharing concepts presented in Section 4 of the Computer Security Incident Handling Guide, Revision 2 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf). The guidance also references the Framework for Improving Critical Infrastructure Cybersecurity” Framework Core, (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf) which is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.

The guide examines the benefits and challenges of coordinating and sharing, presents the strengths and weaknesses of a variety of information sharing models, explores the importance of trust, and addresses specific data handling considerations.

Appendix A provides a collection of scenarios that demonstrate the value of information sharing by describing real-world applications of threat intelligence sharing and coordinated incident response. These include an email phishing attack on people who attended a conference and how an investigation by credit card companies revealed that a retailer was unknowingly under attack.

Read the rest here:
Request for Chapter Presenters

We are well over half way through the year and, we will continue to talk to potential sponsors however due to tighten budgets, they have not been available. As such we are looking for members to present at both the lunch and dinner meeting. The presenter has about 40 minutes to give the presentation and answer questions. This could be one slide with a situation identified and audience will then discuss possible solutions or a how-to presentation with a demonstration afterwards. The below listed are topics that have been suggested as areas of interest from our members. Please send an email to either, Pat Laverty (plaverty1961@gmail.com) and/or myself, Cindy Thornburg (thornbuc@aol.com) with topic to be presented, and we will connect with you for your availability. We would like the topic to be presented at both meetings however we do understand that may be difficult to accomplish.

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

Thank you!

Cindy
The Putin administration has effectively given its blessing to cyber attacks on Western banks and retailers, according to Mandiant founder Kevin Mandia.

The former Pentagon man, whose firm exposed Shanghai-based PLA Unit 61398 last year as the source of prolific hacking activity, said Russia had stepped up its activity of late.

"The Russians are much more aggressive right now across the board – both government and criminal elements – and we’re having a tough time distinguishing between the two," he told the Australian Financial Review from Canberra.

"It stretches credulity that Russian law enforcement and intelligence services, who monitor a hell of a lot of what their people do online, are not aware of what Russian hackers are doing," he added, saying that he was “certain the Russian government was condoning the compromises.”

Just a fortnight ago, Mandiant company FireEye released a new intelligence report detailing the activities of APT28. This new state-sponsored group has apparently been in operation since 2007 and is focused on geopolitical targets like Eastern European governments and NATO that betray Moscow’s hand.

Russian hackers are also thought to be behind the BlackEnergy attacks on US industrial control systems outlined by the ICS-CERT a fortnight ago.

Chris McIntosh, CEO of comms firm ViaSat UK, argued that the threat to CNI has grown as more systems become internet connected.

"The most effective approach now that the threat has been detected is to assume all IT security measures have already been compromised and working backwards on this basis," he added.

"This forms part of a holistic approach to ensure that information is secure from point to point; that workers have peace of mind that they are not putting the organization, themselves or customers at threat and that organizations can be confident that their IT risks have been mitigated.”

News has also emerged that the Russian defense ministry may be throwing up to $500 million at a recruitment drive for a new division of the army focused on cyber threats.

Read the rest here:
A $10 billion-a-year effort to protect sensitive government data, from military secrets to Social Security numbers, is struggling to keep pace with an increasing number of cyber attacks and is unwittingly being undermined by federal employees and contractors.

Workers scattered across more than a dozen agencies, from the Defense and Education departments to the National Weather Service, are responsible for at least half of the federal cyber incidents reported each year since 2010, according to an Associated Press analysis of records.

They have clicked links in bogus phishing emails, opened malware-laden websites and been tricked by scammers into sharing information. One was redirected to a hostile site after connecting to a video of tennis star Serena Williams. A few act intentionally, most famously former National Security Agency contractor Edward Snowden, who downloaded and leaked documents revealing the government’s collection of phone and email records.

Then there was the federal contractor who lost equipment containing the confidential information of millions of Americans, including Robert Curtis of Monument, Colorado.

“I was angry, because we as citizens trust the government to act on our behalf,” he said. Curtis, according to court records, was besieged by identity thieves after someone stole data tapes that the contractor left in a car, exposing the health records of about five million current and former Pentagon employees and their families.

At a time when intelligence officials say cybersecurity now trumps terrorism as the No. 1 threat to the U.S. — and when breaches at businesses such as Home Depot and Target focus attention on data security — the federal government isn't required to publicize its own brushes with data loss.

Last month, a breach of unclassified White House computers by hackers thought to be working for Russia was reported not by officials but The Washington Post. Congressional Republicans complained even they weren’t alerted to the hack.

"It would be unwise, I think for rather obvious reasons, for me to discuss from here what we have learned so far," White House press secretary Josh Earnest later said about the report.

To determine the extent of federal cyber incidents, which include probing into network weak spots, stealing data and defacing websites, the AP filed dozens of Freedom of Information Act requests, interviewed hackers, cybersecurity experts and government officials, and obtained documents describing digital cracks in the system.

That review shows that 40 years and more than $100 billion after the first federal data protection law was enacted, the government is struggling to close holes without the knowledge, staff or systems to outwit an ever-evolving foe.

"It's a much bigger challenge than anyone could have imagined 20 years ago," said Phyllis Schneck, deputy undersecretary for cybersecurity at the Department of Homeland Security, which runs a 24/7 incident-response center responding to threats.

Fears about breaches have been around since the late 1960s, when the federal government began shifting its operations onto computers. Officials responded with software designed to sniff out malicious programs and raise alarms about intruders.

And yet, attackers have always found a way in. Since 2006, there have been more than 87 million sensitive or private records exposed by breaches of federal networks, according to the nonprofit Privacy Rights Clearinghouse, which tracks cyber incidents at all levels of government through news, private sector and government reports.

By comparison, retail businesses lost 255 million records during that time, financial and insurance services lost 212 million and educational institutions lost 13 million. The federal records breached included employee usernames and passwords, veterans’ medical records and a database detailing structural weaknesses in the nation’s dams.

Read the rest here:
NotCompatible botnet infects Android mobiles, infiltrates corporate networks

By Doug Drinkwater, SC Magazine, November 19, 2014

In a new whitepaper released today, the San Francisco-based security company details how it has been tacking NotCompatible and the cyber-criminals behind the threat since early 2012, when the company first revealed it as ‘relatively simple piece of malware’ disguised as an Android system update which turned infected devices into TCP proxies that could be controlled by attackers.

However, the firm says that the group has now released a new and more sophisticated variant – NotCompatible C – which borrows features commonly found in PC malware. For example, the botnet is resilient to network-based blocking as it uses P2P and has multiple geographically-distributed C&C servers (making it difficult for government agencies to takedown), while it encrypts all C2 and proxied data traffic end-to-end.

The malware performs mutual authentication between clients and C2 servers via public key cryptography and has protocol-level encryption which prevents network security systems from differentiating malicious and legitimate traffic. For example, SSL data is sent over port 443 – the default SSL port.

The botnet is certainly more advanced than its predecessor, which had simple client-server architecture where the device communicated directly with one C2 at a time and which employed no encryption or obfuscation to hide the activity. The original NotCompatible carried out “drive-by-download” attacks where victims were served malicious apps when they visited certain websites.

NotCompatible C is able to infect Android devices not through the usual way of fake or Trojanised apps on Google Play, but rather by sending huge quantities of spam to mobile devices which often lack any sort of security protection.

The devices most under threat, according to the firm, are devices which operate outside the traditional security perimeter. These include Bring Your Own Device smartphones and tablets and hand-held inventory scanners. On the latter, Lookout says hackers have already used such a device to bypass security defences and steal a company’s entire financial database.

Once the mobile device is infected, security researchers say that NotCompatible C can be used by attackers to access any network said device was already connected to, such as corporate Wi-Fi networks and VPNs. Fortunately, Lookout traffic suggests that NotCompatible.C clients are connecting to ‘generic’ private networks with no evidence suggesting automatic network scanning.

That said, the firm has not yet analysed traffic from infected devices on potentially targeted corporate networks and instead says that it’s mostly being used to send huge quantities of spam and bypass ecommerce and anti-fraud mechanisms, bulk ticket purchasing and brute force attacks (such as password guessing on WordPress) and c99 control.

But worryingly, the group says that “a large, multi-faceted cyber-crime group” is providing access to its network to other cyber-crime groups” although it says attribution is tricky as NotCompatible was ‘literally built to obfuscate people’s identities’.

The company concluded in its research: “NotCompatible.C possesses distinctive and impressive technical sophistication in the world of mobile malware. Its resiliency, resistance to network-based detection, and self-protection features make it a potent threat in the hands of an attacker. As a mobile botnet with widespread distribution and proxy capabilities, the potential use of NotCompatible.C as a gateway to attack protected networks and systems is not only plausible, but a likely outcome.”

“We believe that NotCompatible is already present on many corporate networks because we have observed, via Lookout’s user base, hundreds of corporate networks with devices that have encountered NotCompatible. It’s reasonable to assume there are many more devices with active NotCompatible infections that are not protected by Lookout that also connect to corporate networks.”

Lookout product manager Jeremy Linden said in an email to SC: “This is the first time Lookout has seen a mobile botnet of this sophistication. The technology has risen to support a robust rent-a-botnet business - something we've seen for years in the PC world, but less so in mobile. People say that mobile threats aren't a problem, but now we're starting to see the sophistication of PC malware on mobile.

Cyber Malware Authors Making a Payday Off Encryption

By Tara Seals, InfoSecurity Magazine, Undated, 2014

Encrypted communications is very en vogue post-Snowden, but there can be unintended consequences. The growing use of encryption to address privacy concerns is creating perfect conditions for cyber-criminals to hide malware inside encrypted transactions, and even reducing the level of sophistication required for malware to avoid detection.

That's the word from Blue Coat Systems, who found in a recent study (http://www.bluecoat.com/documents/download/60ae9a54-4ff0-42c4-8eef-9da13e25fc68) that encryption enables threats to bypass network security and allows sensitive employee or corporate data to leak from anywhere inside the enterprise. That's because encryption makes communications private—and the lack of visibility into SSL traffic represents a potential vulnerability in many enterprises where benign and hostile uses of SSL are indistinguishable to many security devices.

"The tug of war between personal privacy and corporate security is leaving the door open for novel malware attacks involving SSL over corporate networks that put everyone’s data at risk," said Hugh Thompson, chief security strategist for Blue Coat, in a statement. "For businesses to secure customer data and meet regulatory and compliance requirements they need the visibility to see the threats hiding in encrypted traffic and the granular control to make sure employee privacy is also maintained."

Overall, the growing use of encryption means many businesses are unable to track the legitimate corporate information entering and leaving their networks, creating a growing blind spot for enterprises. In fact, over a 12-month period beginning September 2013, between 11% and 14% of the security information requests that Blue Coat researchers received on average each week were asking about encrypted websites. And in a typical seven-day period, Blue Coat Labs receives over 100,000 requests from customers for security information about sites using HTTPS encryption protocol for command and control of malware.

Malware attacks, using encryption as a cloak, do not need to be complex because the malware operators believe the encryption prevents the enterprise from seeing the attack, Blue Coat said. So, significant data loss can occur as a result of malicious acts by hostile outsiders or disgruntled insiders, who can easily transmit sensitive information.

Blue Coat noted that one example of an unsophisticated malware threat hiding in encrypted traffic is Dyre, a widely distributed, password-stealing trojan originating in the Ukraine. "After authorities shut down Zeus, one of the most successful Trojan horse malwares, Dyre quickly took its place by simply adding encryption," the firm noted. "Today, Dyre exploits human behavior to target some of the world’s largest enterprises to compromise accounts that can expose Social Security numbers, bank account information, protected health information, intellectual property and much more."

Read the rest here: http://www.infosecurity-magazine.com/news/malware-authors-making-a-payday/
The Future of Incident Response

By Bruce Schneier, originally appeared in IEEE Security & Privacy, November 10, 2014

After a security incident is detected tremendous resources are spent in the forensic investigation trying to figure out what exactly happened and what data, if any, was compromised. If the forensic investigation doesn’t yield definitive results fairly quickly the organization is left with no choice but to assume the worst.

Security is a combination of protection, detection, and response. It's taken the industry a long time to get to this point, though. The 1990s was the era of protection. Our industry was full of products that would protect your computers and network. By 2000, we realized that detection needed to be formalized as well, and the industry was full of detection products and services.

This decade is one of response. Over the past few years, we’ve started seeing incident response (IR) products and services. Security teams are incorporating them into their arsenal because of three trends in computing. One, we’ve lost control of our computing environment. More of our data is held in the cloud by other companies, and more of our actual networks are outsourced. This makes response more complicated, because we might not have visibility into parts of our critical network infrastructures.

Two, attacks are getting more sophisticated. The rise of APT (advanced persistent threat)--attacks that specifically target for reasons other than simple financial theft--brings with it a new sort of attacker, which requires a new threat model. Also, as hacking becomes a more integral part of geopolitics, unrelated networks are increasingly collateral damage in nation-state fights.

And three, companies continue to under-invest in protection and detection, both of which are imperfect even under the best of circumstances, obling response to pick up the slack.

Way back in the 1990s, I used to say that "security is a process, not a product." That was a strategic statement about the fallacy of thinking you could ever be done with security; you need to continually reassess your security posture in the face of an ever-changing threat landscape.

At a tactical level, security is both a product and a process. Really, it's a combination of people, process, and technology. What changes are the ratios. Protection systems are almost technology, with some assistance from people and process. Detection requires more-or-less equal proportions of people, process, and technology.

Response is mostly done by people, with critical assistance from process and technology.

Usability guru Lorrie Faith Cranor once wrote, "Whenever possible, secure system designers should find ways of keeping humans out of the loop." That's sage advice, but you can't automate IR. Everyone's network is different. All attacks are different. Everyone's security environments are different. The regulatory environments are different. All organizations are different, and political and economic considerations are often more important than technical considerations. IR needs people, because successful IR requires thinking.

This is new for the security industry, and it means that response products and services will look different. For most of its life, the security industry has been plagued with the problems of a lemons market. That's a term from economics that refers to a market where buyers can't tell the difference between good products and bad. In these markets, mediocre products drive good ones out of the market; price is the driver, because there's no good way to test for quality. It's been true in anti-virus, it's been true in firewalls, it's been true in IDSs, and it's been true elsewhere. But because IR is people-focused in ways protection and detection are not, it won't be true here. Better products will do better because buyers will quickly be able to determine that they're better.

The key to successful IR is found in Cranor's next sentence: "However, there are some tasks for which feasible, or cost effective, alternatives to humans are not available. In these cases, system designers should engineer their systems to support the humans in the loop, and maximize their chances of performing their security-critical functions successfully." What we need is technology that aids people, not technology that supplants them.

The best way I've found to think about this is OODA loops. OODA stands for "observe, orient, decide, act," and it's a way of thinking about real-time adversarial situations developed by US Air Force military strategist John Boyd. He was thinking about fighter jets, but the general idea has been applied to everything from contract negotiations to boxing--and computer and network IR.

Speed is essential. People in these situations are constantly going through OODA loops in their head. And if you can do yours faster than the other guy--if you can "get inside his OODA loop"--then you have an enormous advantage.

Read the rest here:
From the November luncheon.

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

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

Article for the Newsletter?
If you would like to submit an article...

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

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

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

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

How the World’s First Computer Was Rescued From the Scrap Heap

By Brendan I. Koerner, Wired, November 25, 2014

Eccentric billionaires are tough to impress, so their minions must always think big when handed vague assignments. Ross Perot’s staffers did just that in 2006, when their boss declared that he wanted to decorate his Plano, Texas, headquarters with relics from computing history. Aware that a few mealy Apple I’s and Altair 880’s wouldn’t be enough to satisfy a former presidential candidate, Perot’s people decided to acquire a more singular prize: a big chunk of ENIAC, the “Electronic Numerical Integrator And Computer.” The ENIAC was a 27-ton, 1,800-square-foot bundle of vacuum tubes and diodes that was arguably the world’s first true computer. The hardware that Perot’s team diligently unearthed and lovingly refurbished is now accessible to the general public for the first time, back at the same Army base where it almost rotted into oblivion.

Read the rest here:
http://www.wired.com/2014/11/eniac-unearthed/