Colleagues,

What a great month August was for our chapter! The Cybersecurity Training Forum (CSTF) was nothing short of outstanding. The number of attendees was higher than anyone had planned for, and we were thrilled to see the local bases represented so well. I really want to thank Glenn York for his outstanding efforts recruiting a diverse group of speakers that was well received by the attendees. In addition, there were so many members who stepped up to help at our table/booth, in speaker rooms, at the welcome desk, and many others who came up and asked where we needed help. Your support made the event a success so thank you.

In September we are back to a lunch meeting on Sept 10th and a dinner meeting on Sept 18th. Our speaker for both events is one of our President Emeritus, Mr. Mark Spencer, so let’s turn out in force to support Mark as he speaks on Risk Management Framework (RMF).

On the 18th of this month we held a board and leadership meeting, and I’m very thankful for the service of all our board members. As a board, we meet every 4-6 weeks to discuss our budget, upcoming events, discuss different things that are going on in the chapter to see if we need additional help in certain areas, etc. This month we discussed lessons learned from the CSTF, discussed our annual recognition luncheon which will be held on the 5th of December at the Antlers Hilton, and discussed our elections to be held at the 5 December luncheon.

Speaking of elections, we know thus far that we have 2 open positions as our recorder Lara Woodworth and our VP of Training Jim Stephens have both notified us they will not be running for reelection. Both Lora and Jim have had huge impacts on this chapter, and their board leadership will be missed, but we are very thankful for all of their efforts. I have asked Colleen Murphy to consider running for the VP of Training, and she has graciously accepted so we know she will be a candidate for this position. Colleen has been leading many of our training events for several years so if elected she would be able to step right in and fill Jim’s very big shoes. I would hope others would consider running as well, though, for any open positions including VP of Training if you are interested.

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.
U.S. firm helped the spyware industry build a potent digital weapon for sale overseas

By Barton Gellman, Washington Post, August 15, 2014

In 2010, elite hackers, most likely from Russia, used at least two zero-day vulnerabilities to penetrate the computer network operated by Nasdaq Stock Market, a hack that allowed them to roam unmolested for months and plant destructive malware designed to cause disruptions, according to a media report published Thursday.

CloudShield Technologies, a California defense contractor, dispatched a senior engineer to Munich in the early fall of 2009. His instructions were unusually opaque.

As he boarded the flight, the engineer told confidants later, he knew only that he should visit a German national who awaited him with an off-the-books assignment. There would be no written contract, and on no account was the engineer to send reports back to CloudShield headquarters.

His contact, Martin J. Muench, turned out to be a former developer of computer security tools who had long since turned to the darkest side of their profession. Gamma Group, the British conglomerate for which Muench was a managing director, built and sold systems to break into computers, seize control clandestinely, and then copy files, listen to Skype calls, record every keystroke and switch on Web cameras and microphones at will.

According to accounts the engineer gave later and contemporary records obtained by The Washington Post, he soon fell into a shadowy world of lucrative spyware tools for sale to foreign security services, some of them with records of human rights abuse.

Over several months, the engineer adapted Gamma’s digital weapons to run on his company’s specialized, high-speed network hardware. Until then CloudShield had sold its CS-2000 device, a multipurpose network and content processing product, primarily to the Air Force and other Pentagon customers, who used it to manage and defend their networks, not to attack others.

CloudShield’s central role in Gamma’s controversial work — fraught with legal risk under U.S. export restrictions — was first uncovered by Morgan Marquis-Boire, author of a new report released Friday by the Citizen Lab at the University of Toronto’s Munk School of Global Affairs. He shared advance drafts with The Post, which conducted its own month-long investigation.

The prototype that CloudShield built was never brought to market, and the company parted ways with Gamma in 2010. But Marquis-Boire said CloudShield’s work helped pioneer a new generation of “network injection appliances” sold by Gamma and its Italian rival, Hacking Team. Those devices harness malicious software to specialized equipment attached directly to the central switching points of a foreign government’s national Internet grid.

The result: Merely by playing a YouTube video or visiting a Microsoft Live service page, for instance, an unknown number of computers around the world have been implanted with Trojan horses by government security services that siphon their communications and files. Google, which owns YouTube, and Microsoft are racing to close the vulnerability.

Citizen Lab’s report, based on leaked technical documents, is the first to document that commercial spyware companies are making active use of this technology. Network injection allows products built by Gamma and Hacking Team to insert themselves into an Internet data flow and change it undetectably in transit.

The report calls that “hacking on easy mode,” in which “compromising a target becomes as simple as waiting for the user to view unencrypted content on the Internet.”

Read the rest here: http://arstechnica.com/security/2014/07/how-elite-hackers-almost-stole-the-nasdaq/
Welcome!

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. August was a great recruiting month with 14 new members. We’ve added 23 new members so far in the third quarter of the year for a total of 81 new members this year. So, everyone, give yourself a 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.

As a separate activity, we are establishing a student mentorship program. Melissa Absher is the chairperson of the Student Mentorship Committee. 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 is looking for more. Thank you to all who have volunteered already. 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

(Continued from page 1)

A Note From Our President

interested. In addition to these two positions, the position of Chapter President and of the Members-At-Large will also be up for re-election. If anyone is interested in any board position, please contact the Chapter VP Cindy Thornburg at Thornbuc@aol.com and Lora Woodworth at woodworth74@gmail.com. This year I would like for all nominees to present themselves at the November Membership meetings so that all our membership has an opportunity to meet candidates and decide who they wish to vote for in December.

Our Executive VP, Tim Hoffman, and I have been speaking recently about having a member serve as a Volunteer Coordinator. For many events, either Cindy or I are coordinating volunteer efforts, and this is spreading us thin at times. We need a member to step up and lead these efforts. So, if you are interested please contact me at plaverty1961@gmail.com or call me at (719) 219-1985; I’d be happy to talk to you about the position.

Sign-ups are going on now for the September meetings. Sign-up will be going out in the first week of September for the October event, and more information will be forthcoming concerning our recognition luncheon. Thanks for all your efforts supporting your chapter, and I’ll see you soon. Cheers.

Pat
The Insider Threat

National Security Institute, Inc., August 21, 2014

Disgruntled employees and other malicious insiders could be one of the most serious security threats faced by companies and nations – but the importance of the threat from the enemy within varies according to whom you ask.

A recent survey of IT security professionals found that only 20% believe insider threats pose the most serious threat to corporate security, with most deeming outsiders a far more serious threat.

That may baffle those who have long feared the insider threat. As it turns out, though, much depends on what you consider a threat. Are we discussing only rogue employees who set out intentionally to steal data? Or do we have to also include careless employees who may cause a breach through laziness or inattention?

It’s an important question, because IT and security executives overwhelmingly agree that employee error and ignorance pose a serious threat to organizations; 44% of the survey respondents say human error is the most frequent point of failure faced by organizations.

And when it comes to man versus machine, it’s not even close: 71% say employees, rather than technology, are the weak link in company security systems.

One researcher said, “I’d have to agree that a very high proportion of security breaches are caused directly or indirectly by people inside an organization, whether it’s a matter of human error, susceptibility to social engineering, or bad security management decisions. I’m not convinced that deliberate malicious action from insiders outweighs all those other factors.”

For workers, the bottom line is this: Know and follow your employer’s security policies, and do your part to make sure your co-workers do as well. If you witness behavior that could put sensitive company information at risk, speak privately about it to your manager.

Before the Internet

---

DO YOU REMEMBER BEFORE THE INTERNET?

OH YEAH, TOTALLY.

WHAT WAS IT LIKE?

NOT HAVING A PHONE OR COMPUTER TO DISTRACT YOU?

YEAH.

IT WAS SO BORING.

ALL THE TIME.

I JUST SAT THERE. IT WAS THE WORST.

BUT WASN’T IT, LIKE, MORE FULFILLING? ENGAGING?

I WOULDN’T KNOW. I STILL GET BORED.

NOT LIKE WE DID.
CSTF Forum Survey Results

By R. Glenn York, CISM, CISSP, CISA, ISSA-COS, August 27, 2014

On August 5th and 6th over 500 people attended the Annual Cyber Security Training Forum (CSTF). We had some great speakers and everyone had a good opportunity to network with other professionals.

While we had a great event this year, we want to improve and ensure we are meeting the needs and expectations of our members and guests so we created a survey about the event and the link was sent to every registered attendee. Some of the questions asked for suggestions for future speakers, vendors, and other improvements. These suggestions are already being considered as we plan to October event and start thinking about the 2015 chapter events. Sixty five people completed the survey. Although this is over 10% of the attendees, we want to hear from everyone to ensure future events meet the needs of all our members and other Information Security professionals in our area. Our goal is to exceed expectations.

The first question on the survey ask to rate the speakers on knowledge, presentation ability and value of content. Over 84% rated the speakers “Above Average” or “Excellent”.

We asked for a rating of our vendors’ knowledge, diversity of products and products or interest. All survey responses rated vendors average or above with over 58% rated “Above Average” or “Excellent”.

We asked if the CSTF 2014 provided a good mix of technical and management presentations. On this question we had over 72% that rated this area “Above Average” or “Excellent”.

On question four we asked everyone to identify the three best speakers they heard at CSFT 2014. Every speaker got at least two votes. The top five speakers based on your votes were Dr. Ron Ross from NIST, BG Kevin Wooton from AFSPC, Michael J. Staggs from Access Data, Robert Bingham from Cyber Dominance Consulting, and Andrea Hoy, from ISSA International.

Although almost everyone attended the CSTF at no cost, we asked people to indicate what they would expect to pay for an event like CSTF. Almost 50% of the responses said $0-$100. Over 23% said they would expect to pay $101-$200 and the rest selected higher price ranges including one that indicated they would expect to pay over $500 for a comparable event.

Although we had 65 people that completed the survey one decided not to indicate if they were an ISSA member of not. This left the other 64 respondents split exactly 50% members and 50% non-members.

As we expected the attendees represented a lot of Federal and DOD employees. The largest single group was Federal Employees with DOD contractors a close second and these two groups represented over 90% of the respondents.

On professional certifications held we had over 66% that hold the Security+ certification with the CISSP a strong second with over 47%. A wide mix of other professional certifications was reported.

Over 50% of the survey respondents indicated they have worked in cybersecurity between 2 and 10 years with slightly less than 25% in the 2-5 year range and just over 25% in the 5-10 year range.

Almost 85% of the respondents had a college degree with 40% holding a Master’s degree and over 50% had completed some graduate school.

Of the people that completed the survey over 70% attended 7 or more sessions which indicates they attended most attended sessions on both days.

When we asked “Why did you attend CSFT 2014?” the largest percentage attended to update their knowledge followed closely by earning CPE credits and networking with other professionals.

Almost 72% of the attendees traveled 1 to 20 miles to the CSTF. Only one person traveled over 150 miles.

If you have suggestions to help make future chapter events better please talk to a chapter board member. We can only get better with your suggestions and involvement in your ISSA Chapter.
Malware Traffic Spikes Preceded Russian and Israeli Conflicts

Government hackers apparently went to work as Israel and Russia ramped up military action this year.

By Tom Simonite, MIT Technology Review, August 26, 2014

A study of malware operating on corporate and government networks suggests that the communication patterns of these programs could warn of major conflicts.

Researchers at the security company FireEye monitored millions of malware messages sent over the past 18 months, and they found spikes in the traffic to and from Russia and Ukraine as tensions rose between the two countries earlier this year. A similar pattern was seen in malware traffic to Israel as it entered its recent hostilities with Hamas.

The FireEye study drew on data collected from more than 5,000 corporate and government clients around the world. FireEye’s software captures “callback” messages sent by malware inside a network—either reporting its status to its operators or picking up new commands. Those messages were used to determine the location of the computer controlling the malware.

The patterns were most likely caused by government agencies ramping up efforts to gather intelligence or attack their adversaries, says Kenneth Geers, who worked on the project. “In the run-up to the Crimea crisis, you saw a rise of malware callbacks in both Russia and Ukraine,” he said at the Black Hat computer security conference Thursday.

It’s also possible that the activity came from hackers sympathetic to but not supported by the countries involved. But many countries now routinely use computer attacks for intelligence and military purposes.

Geers said that patterns in malware communications could be used to predict when countries are preparing for conflict: “If the U.S., or Korea, or Japan was about to go to war, you would see a bump in callbacks—it’s just part and parcel of today’s national security undertakings.” Geers, who recently left FireEye to work as an independent consultant, previously worked on international computer security at the National Security Agency and NATO.

Malware operators sometimes hide their location by having callback messages hop between computers in different countries, and the FireEye study could log only the first hop. However, malware authors don’t always bother to install a system of relays, said Geers. And so, he said, with a large enough data set, accurate geographical patterns emerge.

Much of the traffic to Israel as it moved to strike against Hamas in the Gaza Strip came from malware installed on computers in Canada and the U.S. “You have an indication that maybe Israeli national security organizations are leveraging infrastructure in Canada and the U.S.,” Geers said.

Matching malware traffic to real-world events might also provide a way to uncover tools being used by nation-states. Some of the traffic coming out of Canada, for example, appeared to come from malware that had never been seen before, which FireEye is now investigating.

FireEye plans to continue the research. “We can see the digital equivalent of troops on the border,” Kevin Thompson, a threat analyst for the company, told MIT Technology Review. “But we’d like to look back at a whole year of data and try to correlate with all the world events in the same period.”

Government use of malware is becoming more common, according to Mikko Hyppönen, chief research officer at F-Secure, who studies malware made and used by nation-states. Countries of all sizes use malware because it is relatively cheap and gets results, he said during a talk at Black Hat on Wednesday. “There are parallels here to the nuclear arms race,” he said. “[But] the power of nuclear weapons was in deterrence, and we don’t have that with cyberweapons.”

Read the rest here:
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!
How Much Is Your Privacy Worth?

Despite the outcry over government and corporate snooping, some people allow themselves to be monitored for money or rewards.

By Winston Ross, MIT Technology Review, August 26, 2014

Anyone paying attention knows that his or her Web searches, Facebook feeds, and other online activity isn’t always safe—be it from the prying eyes of the NSA or those of the companies providing a social networking service.

While a substantial chunk of the populace finds all this tracking creepy and invasive, though, there’s a demographic that collectively shrugs at the notion of being mined for data.

Some startups hope to exploit this by buying access to your Web browsing and banking data. Luth Research, a San Diego company, is now offering companies an unprecedented window into the private digital domains of tens of thousands of people who have agreed to let much of what they do on a smartphone, tablet, or PC be tracked for a $100 a month.

Luth’s “QZ Intelligence” service collects and analyzes data from preselected participants’ phones and computers via a virtual private network connection. Data is routed through the company’s servers where it is collected and analyzed for trends. The company doesn’t view the contents of messages, but what it does gather includes where smartphone users are at any given moment, what websites they are visiting, what queries they are feeding into Google, and how often they check Twitter. The program’s participants are also asked to answer questions about their behavior.

Luth’s current and former clients include Subway, Microsoft, Walmart, the San Diego Padres, Nickelodeon, and Netflix. The information it collects can help companies decide where to spend advertising dollars. Advertisers want better targeting because click-through rates for online ads now stands at less than .01 percent.

Luth did a project for Ford Motor Company this year—Ford wanted to better understand customers’ “path to purchase.” The company rounded up research subjects in the market for a car, and then tracked the journey they took from researching to finally buying. A customer might drive to a dealership, browse other automakers’ websites while there, and research financing options later. All of that behavior can be analyzed to help Ford figure out where to best spend its advertising dollars. If it turns out that consumer review sites are a prominent part of the process, for instance, Ford can focus on commissioning reviews, partnering with the sites, and buying ads there.

Ultimately, Luth found that by the time a customer actually visits a car manufacturer’s website, they’re most likely ready to buy a car. “That’s a big deal,” says the company’s senior executive for marketing, Becky Wu. “We didn’t know that until this project. If you know that person is really ready to buy, it’s a hot lead.”

Read the rest here:

Digital Clues Leading the Hunt for ISIS Killer

By Jill Lawless, Associated Press, August 22, 2014

The Islamic militant in a video showing the death of American journalist James Foley took great care to disguise his identity, dressing head-to-toe in black, with a mask leaving only his eyes visible.

But police and intelligence services in Britain and the United States have a plethora of clues as they scramble to identify him, from image analysis and voice-recognition software to social media postings and testimony from former captives.

Prime Minister David Cameron has said the masked jihadi pictured holding a knife to Foley's throat is likely British, and linguists say his accent suggests he is from the London area.

Britain's Metropolitan Police is involved in the hunt for him, as are British intelligence agencies and the FBI.

The Guardian newspaper on Thursday quoted an unnamed former captive who was held by the Islamic State group in Raqqa, Syria, as saying he appeared to be one of several British militants — nicknamed "The Beatles" by hostages — charged with guarding prisoners.

Peter Neumann, director of the International Center for the Study of Radicalization at King’s College London, said it was likely Foley's beheading had taken place in Raqqa, a stronghold of the Islamic State militant group and the base for many of its foreign fighters.

He said investigators would use basic detective techniques to narrow down the field of suspects before turning to voice recognition software and other sophisticated technology.

Neumann said most of the hundreds of Western militants in Syria have Facebook or Twitter accounts, on which they post pictures of themselves and give away other clues to their origins, such as a favorite soccer team.

Read the rest here:
http://www.net-security.org/secworld.php?id=17150
Military Companies Brace for Rules on Monitoring Hackers

By Chris Strohm, Bloomberg, August 13, 2014

Companies that do business with the Defense Department are bracing for new U.S. rules requiring them to report computer breaches to the Pentagon and give the government access to their networks to analyze the attacks.

Groups representing the contractors are raising concern about the Pentagon rooting around their data, and say smaller companies may not even have the cybersecurity protections needed to comply. A report that was to be released today on the rules has been pushed back until Sept. 24, according to a person familiar with the matter who isn’t authorized to speak publicly.

The pending rule change marks an escalation of efforts to understand the scale of hacking as the Defense Department plans to spend $23 billion through fiscal year 2018 on cybersecurity. The crux of the rule is designed to ensure companies handling classified data quickly inform the Pentagon of hacking attacks.

The effort “has the potential to become too onerous” if it requires contractors to report minor breaches and allows the Pentagon access to trade secrets or personal information on their networks, said Mike Hettinger, senior vice president for the public sector at TechAmerica, a trade association based in Arlington, Virginia, that represents Lockheed Martin Corp. (LMT), Northrop Grumman Corp. (NOC) and other defense contractors.

“The idea is to make sure we know where these breaches have been and protect information that is in these systems, and not just make people disclose for disclosure’s sake,” Hettinger said in an interview.

Congress mandated the rules as part of a budget authorization measure in 2013 for the Defense Department after repeated warnings from Pentagon officials about hacking threats and successful incursions.

Business Costs

The 2013 law had called for the rules to be developed within 90 days.

Foreign hackers stole 24,000 U.S. military files in a single incident on a defense contractor in March 2011 in one of the Pentagon’s worst cyber-attacks. In May 2011, Bethesda, Maryland-based Lockheed suffered what it called a “tenacious” attack on its computer networks, though the company said no employee, program or customer data was lost.

“Cybersecurity is increasingly becoming the cost of doing business with the federal government,” Daniel Stohr, director of communications for the Aerospace Industries Association, said in a phone interview. “It’s something as an industry that we have to face.”

Clear Guidance

The rules could have a far-reaching impact on small and medium-sized companies and their vendors, though the exact cost is impossible to know without the details, said Rusty Rentsch, assistant vice president for technical operations at the Arlington, Virginia-based association, which represents almost 150 companies including Boeing Co. (BA) and DigitalGlobe Inc. (DGI)

Companies will be looking for clarity about what kind of breaches have to be reported and what procedures need to be followed when incursions are found, Rentsch said in a phone interview.

“We’re looking for clear guidance on how to implement whatever requirements the government is looking to put into place,” he said. “We don’t want contracting officers giving their personal interpretation of what this rule would or should be.”

Companies also will want the Pentagon to share information about hacking threats in order to help them better understand what to watch for, Rentsch said.

Hacking risks are growing and top the list of global threats, Director of National Intelligence James Clapper told the Senate’s intelligence committee in January. It was the second year in a row that hacking threats were the top concern.

Uniform Standards

A report last month from the federal commission that investigated the Sept. 11, 2001, terrorist attacks said cybersecurity is “the battlefield of the future” and the nation’s ability to protect core networks lags far behind the growing threat.

The rules will apply to contractors that have Pentagon security clearances to access, receive, or store classified information for the purpose of bidding on a contract or conducting activities in support of programs, according to language that lawmakers wrote to accompany the 2013 defense authorization bill.

Contractors must report a description of methods used in an attack and provide a sample, if found, of the malicious software used, according to the lawmakers.

Heartbleed is the gift that keeps on giving as servers remain unpatched

An average of 7,000 attacks continue to seek out servers vulnerable to the bug.

By Robert Lemos, ArsTechnica, August 28, 2014

Within four days of the first public reports of a major flaw in OpenSSL's software for securing communications on the Internet, mass attacks searched for and targeted vulnerable servers.

In a report released this week, IBM found that while the attacks have died down, approximately half of the original 500,000 potentially vulnerable servers remain unpatched, leaving businesses at continuing risk of the Heartbleed flaw. On average, the company currently sees 7,000 daily attacks against its customers, down from a high of 300,000 attacks in a single 24-hour period in April, according to the report based on data from the company's Managed Security Services division.

"Despite the initial rush to patch systems, approximately 50 percent of potentially vulnerable servers have been left unpatched—making Heartbleed an ongoing, critical threat," the report stated.

The Heartbleed flaw, disclosed on April 9, allows attackers to request 64KB of the most current data from an affected server that uses OpenSSL. In many cases, the data could be nonsensical digital garbage, but in others, an attacker could mine cryptographic keys and passwords by exploiting the flaw.

That's just what attackers began to do on April 11, hitting hundreds of IBM's clients with 200,000 daily attacks. By April 15, attack events peaked at 300,000 and then quickly dropped off. Ten days after the initial wave of attacks, the number of events had dropped to the thousands.

The Heartbleed vulnerability has highlighted a number of problems with how companies and the security community address software security problems, IBM stated. While Heartbleed is considered one of the most critical bugs impacting the Internet in 2014, a common measure of vulnerability severity—the Common Vulnerability Scoring System, or CVSS—only rated the issue a 5.0, or "medium," threat.

In addition, companies that had incident response plans prepared and closely managed their information-technology assets were able to patch quickly. Without both, responding to Heartbleed took much longer, IBM stated in the report.

Read the rest here: http://arstechnica.com/security/2014/08/heartbleed-is-the-gift-that-keeps-on-giving-as-servers-remain-unpatched/

How good is your agency's incident response?

By William Jackson, GCN, August 25, 2014

As in any job, in cybersecurity it's the paperwork that gets you. In a recent study, the Government Accountability Office found that agencies are doing an incomplete job in documenting their response to security incidents.

The GAO studied a sample of 40 incidents in fiscal 2012 at six agencies to get a statistical picture of overall practices at 24 major executive branch agencies. In about 65 percent of the cases, it found that incident response activities were not fully documented.

Most agencies identified the scope of the incident, but often did not demonstrate that they knew the impact of it. Other responses, such as actions to prevent recurrence of an incident, often were not shown. Each of the agencies studied had some type of an incident response plan, but none was comprehensive.

The Office of Management and Budget and the Department of Homeland Security oversee agencies' cybersecurity activities, but neither had addressed incident response practices in their CyberStat reviews.

These shortfalls come at a time of increasing rates of Cyber incidents at agencies, from 34,840 in fiscal 2012 to 46,160 in fiscal 2013.

Read the rest here: http://gcn.com/articles/2014/08/25/hspd-12-documentation.aspx?admgarea=TC_SEC_CybersSec
Why Offender Profiling is Changing Thanks to Mobile Forensics and Increasingly ‘Social’ Criminal Activity

By Yuval Ben-Moshe, Forensic Focus, August 26, 2014

Law enforcement agencies across the globe are taking a page out of the cybercriminal handbook, using targets’ own phones and computers to spy on them with methods traditionally associated with the world’s most malicious hackers, two computer security groups say.

Mobile forensics has changed the methodology when it comes to offender profiling. The frequent use of mobile devices has provided investigators with another source for profiling criminal suspects, as well as an insight into their habits and personalities.

This is not just because of the volume of user voice calls and SMS texts; the amount of rich data that can be extracted from Instant Messaging (IM) and social media applications gives forensic investigators the paint and brushes to develop a detailed picture of a suspect and a criminal case. A suspect’s social media personality can offer a more tailored overview of the character, his or her likes and dislikes and a reflection of ‘who’ they really are, beyond their alleged actions. A victim’s presence on social media can also be used to find a common link to possible suspects.

Recent research from Cellebrite found that 77 per cent of respondents believed that mobile apps were a critical data source in criminal investigations. While this clearly indicates that mobile apps offer a vital source of evidence, it’s not a suggestion that investigators should solely look at mobile-based apps when building the investigative picture – evidence should be extracted from all other items of phone-based data as well.

The widespread use of mobile apps makes them a critical data source for law enforcement, both in terms of evidence and investigative leads. The value to both prosecuting and defence counsels, in a court of law, makes the neglect of such data a potentially severe barrier to solving a case.

People now more frequently use mobile devices to access social media apps, rather than using a traditional PC or laptop. Moreover, social media data that is extracted from a suspect’s mobile device provides additional characteristics such as more accurate location-based data and time proximity to another event or situation. For example, by connecting to a specific Wi-Fi network investigators can establish presence in a certain place and at a certain time correlating it with another action, possibly, on social a network.

Criminals will use various communication channels in the course of their mobile activity. For example, a suspect could use an IM app to organise a meeting, but use SMS to contact the victim. Investigators must operate a flexible forensic practice when sourcing evidential data from mobile devices, because the various channels that criminals communicate through means that a one dimensional approach to forensic evidence gathering could lead to the omission of valuable data.

While data points such as SMS text messages and GPS locations may result in an immediate lead in a criminal case, the ‘online social identity’ of a suspect will allow investigators to delve into the personality of the suspect, which in turn could help build out the case.

This social data can be extracted through the social media apps that the suspect has downloaded on their device. Facebook posts, Tweets, ‘shares’ and ‘likes’ can all give critical information to investigators hoping to build the profile of a suspect.

A suspect’s social media identity goes beyond their ‘likes’ and ‘shares’ though; it can also include immediate locational data, such as a recent ‘check-in’ at a restaurant or a shop. Even if this locational data isn’t completely current, it will still help to paint the forensic picture of a suspect in terms of where they regularly go, who they meet with, and what they do when they’re there.

In court, social data retrieved from mobile apps is fast-becoming a major source of evidence in not only building up the profile of the suspect, but also in establishing or demolishing a witness’ credibility. While social or app-based data has become a crucial evidential component to an investigator’s case, it can also act as an important part of the prosecution or defence process in court.

Offender profiling is changing as people use more social applications to communicate with one another. This is providing investigators with another source of information to build up a complete profile of a suspected criminal, which in turn offers a more comprehensive picture of a suspect in a court of law.

Read the rest here:
http://articles.forensicfocus.com/2014/08/26/offender-profiling-is-taking-a-different-shape-as-investigators-grapple-with-
By Clifford Atiyeh, Popular Mechanics, August 22, 2014

The explosive growth in both the use and capacity of smartphones has led to a sea change in digital forensics, creating technology challenges for the justice and law enforcement communities and raising legal questions that in some cases have gone to the Supreme Court.

Computer hackers, call off your salvos against Microsoft and stop trying to wreck our blog: Break into a Model S and Tesla might hire you.

The electric automaker wants to hire up to 30 full-time employees from the hacking community, as evidenced from its display at the recent annual Def Con conference in Las Vegas. More than 10,000 coders and network-security pros (the nice people who point out digital flaws without destroying the whole world) gathered there to brush up on their skills, including demonstrating control over hotel elevators. If you don’t speak l33t, you don’t attend Def Con.

Tesla wants more programmers to find security holes in its cars, all of which come with internet connections, perform over-the-air software updates, and have an infotainment screen the size of a Times Square billboard that is used to control everything from navigation to the door locks. Although the Def Con event wasn’t a Tesla “hackathon” like what happened in China—there, hackers took control of the car’s sunroof, lights, and horn—it did allow Tesla to recruit experts for what may become the biggest electronics-security team in the auto business. Interns are being sought, too, and anyone who finds a flaw gets mentioned on the Tesla website (there are 20 such mentions at present) and can win “challenge coins” for free factory tours in Fremont, California.

Tesla’s own “hacker princess,” former Apple and Microsoft employee Kristin Paget, told the Wall Street Journal that the firm had patched at least one security hole in the Model S reported by an outside hacker. Tesla wouldn’t confirm whether it had actually hired anyone from Def Con.

Read the rest here:

Okay, it’s a three day weekend so I thought I would give you a quick glimpse behind the scenes at the ISSA-COS Newsletter.
The surge of Web-connected devices—TVs, refrigerators, thermostats, door locks and more—has opened up huge opportunities for cyberattacks because of weak security, researchers said Tuesday.

During his keynote and a press conference that followed here at the Black Hat information security conference, In-Q-Tel Chief Information Security Officer Dan Geer expressed concern about the growing threat of botnets powered by home and small office routers. The inexpensive Wi-Fi routers commonly used for home Internet access—which are rarely patched by their owners—are an easy target for hackers, Geer said, and could be used to construct a botnet that "could probably take down the Internet." Asked by Ars if he considered home routers to be the equivalent of critical infrastructure as a security priority, he answered in the affirmative.

Geer spoke about the threat posed by home routers in advance of "SOHOpelessly Broken," a router hacking contest scheduled for the DEF CON security conference later this week sponsored by the Electronic Frontier Foundation. "Because they are so cheap, you can get a low-end router for less than 20 bucks that hasn't been updated in a while," Geer explained. Attackers could identify vulnerabilities in particular models and then scan the Internet for targets based on the routers' signatures. "They can then build botnets on the exterior of the network—the routing that it does is only on side facing ISPs," he said. "If I can build a botnet on the outside of the routers, I could probably take down the Internet."

During his keynote, Geer had said that inexpensive routers were an example of the security risk of the "Internet of Things," because of their use of long-lived embedded software with no automatic way for vendors to distribute patches. "All embedded software should either have a remote management interface, or they need a finite lifetime," he opined, "because if they live long enough, something bad will happen. If a person lives long enough, they will get dementia—if a piece of software lives long enough, it will be taken over."

2014 Annual Cyber Security Training Forum
ISSA photos are courtesy of our Chapter photographer Warren Pearce.
The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

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

### 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 to Use Your Cat to Hack Your Neighbor’s Wi-Fi

By Andy Greenberg, Wired, August 8, 2014

Late last month, a Siamese cat named Coco went wandering in his suburban Washington, DC neighborhood. He spent three hours exploring nearby backyards. He killed a mouse, whose carcass he thoughtfully brought home to his octogenarian owner, Nancy. And while he was out, Coco mapped dozens of his neighbors’ Wi-Fi networks, identifying four routers that used an old, easily-broken form of encryption and another four that were left entirely unprotected.

Unbeknownst to Coco, he’d been fitted with a collar created by Nancy’s granddaughter’s husband, security researcher Gene Bransfield. And Bransfield had built into that collar a Spark Core chip loaded with his custom-coded firmware, a Wi-Fi card, a tiny GPS module and a battery—everything necessary to map all the networks in the neighborhood that would be vulnerable to any intruder or Wi-Fi mooch with, at most, some simple crypto-cracking tools.