Upcoming Cyber Training Forum!

Colleagues,

Summer is upon us and I hope all of you take some time to enjoy the warm weather while it lasts. As a chapter, I’m very pleased

As I write this we are well into our planning for the Cyber Security Training Forum (CSTF). For those who are unfamiliar with this conference, for many years our chapter has partnered with Federal Business Council in an effort to provide Colorado Springs security and IT professionals an opportunity to hear from Department of Defense and Industry Leaders as well as other knowledgeable people in our profession. This year the CSTF is 5-6 August at the Doubletree Hotel. Entrance to the CSTF is FREE if you go to http://www.fbcinc.com/e/cstf and use the code CSTF14ISSA. In addition, it is free for government (military and civilian) employees so please help get the word out. Our keynote speaker is Dr. Ron Ross. Dr. Ross is the principal architect of the Risk Management Framework and he also leads the Joint Task Force Transformation Initiative, a partnership with NIST, the Department of Defense, the Intelligence Community, the Office of the Director National Intelligence, and the Committee on National Security Systems to develop a unified information security framework for the federal government. Glenn York has been leading our chapters efforts to get exceptional speakers and leaders to speak at the conference and Dr Ross is a headliner...we really look forward to hearing from him.

Halfway through the year our chapter is doing very well. We have had 9 chapter meetings thus far in 2014 as well as a conference held at UCCS with over 200
We “will be paying no ransom,” vows town hit by Cryptowall ransom malware

By Dan Goodin, ArsTechnica, June 7, 2014

The town manager of a hamlet in southeastern New Hampshire has defied demands that he pay a ransom to recover police department computer files taken hostage by Cryptowall, a newer piece of malware that encrypts hard drive contents of infected machines until victims pay for them to be decrypted.

"Make no mistake, the Town of Durham will be paying no ransom," Town Manager Todd Selig was quoted as saying by CBS Boston news. Police department computers for the town of almost 15,000 residents were reportedly infected Thursday after an officer opened what appeared to be a legitimate file attachment to an e-mail. By Friday morning, widespread "issues" were hitting the department computer network. It was shut down by noon that day to prevent the infection from spreading to other systems.

The game may be RIGged

The department was reportedly hit by Cryptowall, a newer form of crypto malware that rivals the better known CryptoLocker. According to a blog post published Thursday by researchers from Cisco Systems, Cryptowall has been gaining ground since April, when it was folded into the RIG exploit kit, which is software sold in underground forums that automates computer scams and malware attacks for less technically knowledgeable criminals. Cisco's Cloud Web Security service has been blocking requests tied to more than 90 infected Internet domains pushing Cryptowall scams to more than 17 percent of service customers.

Contrary to reports that the Durham Police Department infection was the result of a malicious e-mail attachment, the RIG-fueled attacks Cisco is blocking are the result of malicious advertisements served on scores of websites, including altervista.org, apps.facebook.com, www.theguardian.com, and ebay.in. The US is the country seeing the most infected ads, followed by the UK. So-called malvertising is a scourge that uses authentic-looking ads served over legitimate networks and sites to either trick end users into clicking on malicious links or to push attack code that exploits vulnerabilities to surreptitiously install malware.

"Until May 22, RIG appears to have been making use of both newly registered domains and compromised legitimate sites to both host its landing pages and serve its exploits, all from paths ending in 'proxy.php,'" the Cisco blog post stated.

The rash of Cryptowall attacks came to light the same week that federal authorities seized a massive botnet used to spread CryptoLocker. The effects of Cryptowall on Durham were characterized as disruptive but not catastrophic.

"The functions affected are the police e-mail system and word processing, as well as spreadsheets, Excel, and other administrative tasks," Selig said. "The crime records are not affected. We do back up all of our systems, so we will work to restore what may be lost."

CryptoLocker underscored the importance not just of backups, but of so-called "cold" backups that are done offline. Because CryptoLocker encrypted files on all accessible drives, it often overwrote backup files as well as original ones. In many cases, backups were intact only when they were stored in offline systems that were protected from the infected computers. The distinction could prove particularly important to Durham residents given the refusal to pay the ransom. According to Cisco, ransom demands sent to a test computer that was infected by Cryptowall were increased three times to $600, after which time the data would be irretrievable.

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. We’ve added 22 new members so far in the second quarter of the year for a total of 58 new members this year. So, everyone, give yourself a pat on the back and continue to bring in new members. We still need at least another 25+ new members to hit our recruiting goal 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. We provided some recommendations to the Chapter Board in June and they agreed to our approach. This will be a student-focused program, separate from the formal ISSA mentorship program. As part of the Membership Committee, we will be forming a Student Mentorship Committee with Melissa Absher as the chairperson. This summer Melissa will begin pulling together some ideas so when our student members return in the fall we can begin meeting with them. Initially, we will be meeting as a group while we determine needs, wants, capabilities, etc. and the program will mature from there. We are very much at the “crawl” stage with this idea right now. We want to ensure that we set reasonable expectations that we can meet so the program will be successful from the students’ perspective. We also want to provide sufficient guidance and support to prospective mentors to ensure their success too. Several of our new UCCS student members have already expressed an interest in having a mentor and we’ll be reaching out to other new student members to see if they are also interested.

We are looking for members to join the Student Mentorship Committee so if you’re interested in mentoring some of our new student members please contact me and I’ll pass your information along to Melissa.

Thanks for all your efforts and support.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

A Note From Our President

attendees. That means you have had, and will continue to have, a lot of opportunities to get your continuing education credits. Our events continue to be well attended and we hope you’ll continue to support your chapter by keeping your membership current, helping recruit new members, and by remaining active. There are several chapter members who are stepping up to provide informative briefings to us and it’s important that we have good turnouts showing them that we appreciate their efforts to help us learn and stay informed.

Hope everyone is enjoying their summer and as always, if you have ideas or suggestions to help our chapter please give me a call at (719) 360-4543 or send me an e-mail to plaverty1961@gmail.com.

Cheers,

Pat

New Members: June
Paulette Iszler
Randall Sykes
Melissa Langlois
Suzanne Chance
Thomas Joyce
Emily Danis
Request for Chapter Presenters

We are almost half way through the year and only had one sponsor so far this year. 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 release of the Risk Management Framework (RMF) methodology in March 2014 may have caught some in the DoD community flat-footed. For many others, the response by those on their toes and immersed in cybersecurity the attitude has been, "It's about time".

Explaining what RMF is and how the security authorization package process is going to work has been a challenge. Policy experts have been trying to get their arms around DoD instructions, CNSS issuances, NIST special publications, and the mandates defined in FIPS publications. In contrast, the intelligence community has ironed-out many of the kinks of the RMF process, and their processes are in motion.

In the Defense community, there seems to be a "calm before the storm" to flesh-out the RMF People, Operations, and Technology aspects (P.O.T. if you like mnemonics). Since there is a policy level six-month pause, it is a ripe time to get prepared. And, remarkably, the POT dimensions really hold the vision for the way-ahead. **PEOPLE** (we) need to take advantage of the training opportunities pertaining to the RMF principles. As we learn the RMF concepts we will have opportunities to help establish the **OPERATIONS** that will replace the old C&A pipeline. Finally, training or OJT is essential to get proficient with the **TECHNOLOGY** - namely, the RMF tools that are being developed or, are already developed. Technology amounts to online programs (enterprise applications) that support RMF to include eMASS for most people, and Xacta for others.

In summary, the common factor for this People - Operations - Technology sandwich is training. And as cybersecurity professionals, we (ultimately) establish the success and efficiency of the RMF Operation; the new pipeline, the RMF pipeline.

The astute practitioner will glean current guidance from every relevant pub, instruction, book, or training class available. In 2009, a seminal work called, "The Definitive Guide to the C&A Transformation" by Dr. Julie Mehan and Waylon Krush, helped digest the doctrines listed above. The book provided many of the early concepts that forged the RMF concept. For the initiated, several hits for "RMF training" can be discovered on Google. The rigor of training and education offered by each course varies widely. Don't set your expectations too high. Due diligence is upon the cybersecurity professional to study. Realistic training course expectations should be to gain a familiarity of the material from the instructor, get the certificate for your resume, and decompress from what might otherwise be a daily grind. And depending on the investment of your continuous studies, you may end-up rubbing shoulders with the best of them.

An example of RMF related training includes several courses that are based on the CNSS instructions. The following are four recommendations:

- **NSTISSI-4011** (National Training Standard for Information Systems Security (INFOSEC) Professionals)
- **CNSSI-4012** (National IA Training Standard for Senior Systems Managers)
- **NSTISSI-4015** (National Training Standard for Systems Certifiers)
- **CNSSI-4016** (National IA Training Standard For Risk Analysts)

Finally, it is commendable to note that the ISSA Colorado Springs chapter has several members who have earned the Risk Analyst certification complying with the CNSSI-4016 standards. Three classes convening in July 2013, September 2013, and June 2014 certified a total of 38 students as Risk Analysts for national security systems.
RMF Training Track

By Kurt Danis, ISSA-COS, June 27, 2014

The Risk Management Framework (RMF) training track is suggested for CyberSecurity staff with the goal to enhance their competencies in support of the RMF methodology. RMF competencies demand adept skills to properly handle technical findings, and deep knowledge abide to high-level policies. The RMF professional should strive to understand the principles and tenants to help their organization embrace the RMF processes and strategies for their systems. The following certifications would be in addition to the CISSP foundation (or equivalent).

**POPULAR ADVANCED CERTIFICATIONS**

- **ISC2’s Certification and Accreditation Professional (CAP) course.** A subset of the ISSEP body of knowledge. $1000 - $2000.
- **SANS’ Global IA Certification (GIAC) Security Leadership Certification (GSCL):** Predicated on completing the SANS Security Leadership Essentials For Managers (MGT 512). $4,645 plus $599 for exam.
- **ISC’s Information System Security Engineering Professional (ISSEP) course:** One week “bootcamp”. $1,500 to $2,800.
- **ISC’s Information System Security Management Professional (ISSMP) course:** One week “bootcamp”. $1,500 to $2,800.
- **ISC’s Information System Security Architecture Professional (ISSAP) course:** One week “bootcamp”. $1,500 to $2,800.
- **ISACA’s Certified Information Security Manager (CISM) course:** $3,000 from Training Camp in Virginia.
- **NSTISSI 4011 National Training Standard for Information Sys. Sec. (INFOSEC) Pros**
- **CNSSI 4012 National IA Training Standard for Senior Systems Managers**
- **CNSSI 4013 National IA Training Standard for System Administrators (SA)**
- **CNSSI 4014 National IA Training Standard for Information Systems Security Officers**
- **NSTISSI 4015 National IA Training Standard for System Certifiers**
- **CNSSI 4016 National IA Training Standard for Risk Analysts:** $1,500, IA2, Inc.

Avoid having too many certifications. Most certs have annual maintenance fees and professional development requirements. The CNSS certs (above) do not have these burdens.

**STRATEGIC CERTIFICATIONS**

The DoD 8570.01-M, Change 3, January 24, 2012 prescribed higher professional requirements to support the more advanced or senior Certification & Accreditation (C&A) functions. Senior C&A roles usually support the program office levels (e.g. SPO, PEO, and others). Expert certifications that may support senior RMF roles include:

- The ISSEP and the ISSAP certifications to qualify people in the IA [workforce] System Architect and Engineer (IASAE) role.
- A CISSP-ISSMP certification to qualify people in the Computer Network Defense-Service Provider (CND-SP) role.

**EXPERT TECHNOLOGY CERTIFICATIONS**

**The Gang of Five**

“The Gang of Five” pertains to certifications relative to five most common network devices. SCA representatives and Security Test & Evaluation (ST&E) professionals should be proficient and capable of testing firewalls, servers, workstations, switches, and routers. Certifications for these network device technologies will demonstrate the necessary competency and validate that a system risk assessment has some merit and legitimacy.

**Expert Technology Certifications to consider:**

- Cisco Certified Network Associate
- Cisco Certified Network Associate Security
- Cisco Certified Design Associate
- Sun Certified Solaris Associate

(Continued on page 7)
$445 billion lost due to cybercrime?

By HelpNet Security, June 9, 2014

Cybercrime has a significant impact on economies worldwide. A new report from the Center for Strategic and International Studies (CSIS) concludes that cybercrime costs businesses approximately $445 billion worldwide (approximately £266 billion), with an impact on approximately 150,000 jobs in the EU and 200,000 jobs in the U.S.

The most important cost of cybercrime comes from its damage to company performance and to national economies. Cybercrime damages trade, competitiveness, innovation, and global economic growth. Studies estimate that the internet economy annually generates between $2 trillion and $3 trillion, a share of the global economy that is expected to grow rapidly. Based on CSIS analysis, cybercrime extracts between 15% and 20% of the value created by the internet.

Cybercrime’s effect on intellectual property (IP) is particularly damaging, and countries where IP creation and IP-intensive industries are important for wealth creation lose more in trade, jobs and income from cybercrime than countries depending more on agriculture or industries of low-level manufacturing, the report found. Accordingly, high-income countries lost more as a per cent of GDP than low-income countries – perhaps as much as 0.9 per cent on average.

“Cybercrime is a tax on innovation and slows the pace of global innovation by reducing the rate of return to innovators and investors,” said Jim Lewis of CSIS. “For developed countries, cybercrime has serious implications for employment. The effect of cybercrime is to shift employment away from jobs that create the most value. Even small changes in GDP can affect employment.”

Economic impact on both businesses and consumers

CSIS researchers found that in the U.K., retailers reportedly lost more than $850 million to hackers. The United States notified 3,000 companies in 2013 that they had been hacked, with retailers leading as a favourite target for hackers. Australian officials reported that large scale attacks have occurred against an airline, hotel chains and financial services companies, costing an estimated $100 million. With proper protections in place, these losses could be avoided.

The report found that global losses connected to “personal information” breaches could reach $160 billion. Forty million people in the U.S., roughly 15 per cent of the population, have had their personal information stolen by hackers. The study tracked high-profile breaches around the world with 54 million in Turkey, 20 million in Korea, 16 million in Germany and more than 20 million in China, having their personal information stolen in the last year.

Part of the losses from cybercrime are directly connected to what experts call “recovery costs,” or the digital and electronic clean-up that must occur after an attack has taken place. The McAfee-CSIS report discovered that while criminals will not be able to monetise all the information they steal, their victims must spend significant resources as if they could.

In Italy, for example, actual hacking losses totaled $875 million, but the recovery, or clean-up costs, reached $8.5 billion. In other words, there can be a tenfold increase between the actual losses directly attributed to hackers and the recovery companies must implement in the aftermath of those attacks.

Read the rest here:
http://www.net-security.org/secworld.php?id=16981

RMF Training Track

(Continued from page 6)

- Linux+ or Linux Professional Institute Level I
- Certified Ethical Hacker
- Oracle Database Administrator Certified Associate
- Sidewinder cert
- Riverbed Accelerators (WANX) cert
- VPN (Juniper, Netscreen)
- IDS / IPS sensor certs

Microsoft Certified Professional (MCP) refers to all certifications by Microsoft. Specific Microsoft Certified (MC) certs include the IT Professional (MCITP), Architect (MCA), Professional Developer (MCPD), Technology Specialist (MCTS), Systems Administrator (MCSA), Systems Engineer (MCSE), Solution Developer (MCSD) and the Database Administrator (MCDBA). The **MCITP, MCSA, and MCSE** are recommended certs for the SCA professional supporting the RMF methodology.

http://en.wikipedia.org/wiki/Microsoft_Certified_Professional
Redmond is patching Windows 8 but NOT Windows 7, say security bods

By Darren Pauli, The Register, June 6, 2014

Microsoft has left Windows 7 exposed by only applying patches to its newest operating systems.

Researchers found the gaps after they scanned 900 Windows libraries and uncovered a variety of security functions that were updated in Windows 8 but not in 7. They said the shortcoming could lead to the discovery of zero day vulnerabilities.

The missing safe functions were part of Microsoft's dedicated libraries intsafe.h and strsafe.h that help developers combat various attacks.

Researcher Moti Joseph (@gamepe) - formerly of Websense - speculated Microsoft had not applied fixes to Win 7 to save money.

"Why is it that Microsoft inserted a safe function into Windows 8 [but not] Windows 7? The answer is money - Microsoft does not want to waste development time on older operating systems ... and they want people to move to higher operating systems," Joseph said in a presentation at the Troopers14 conference.

Microsoft has been contacted for comment.

Together with malware analyst Marion Marschalek (@pinkf1awd), the duo developed a capable differencing (comparison) tool dubbed DiffRay which would compare Windows 8 with 7, and log any safe functions absent in the older platform.

It was "scary simple", Marschalek said, and faster than finding vulnerabilities by hand.

Security bods could then probe and pluck those functions to identify vulnerabilities and exploits.

In a demonstration of DiffRay, the researchers found four missing safe functions in Windows 7 that were present in 8.

"If we get one zero-day from this project, it's worth it," Joseph said.

Read the rest here:
http://www.theregister.co.uk/2014/06/06/patch_piker_redm ond_means_win_8_fixes_skip_7_researchers_say/

Knock-off Smartphone Sends Info Back to China

By Raphael Satter and Frank Jordans, Associated Press, June 19, 2014

A cheap brand of Chinese-made smartphones carried by major online retailers comes preinstalled with espionage software, a German security firm has said.

G Data Software said it found malicious code hidden deep in the propriety software of the Star N9500 when it ordered the handset from a website late last month. The find is the latest in a series of incidents where smartphones have appeared preloaded with malicious software.

G Data spokesman Thorsten Urbanski said his firm bought the phone after getting complaints about it from several customers. He said his team spent more than a week trying to trace the handset's maker without success.

"The manufacturer is not mentioned," he said. "Not in the phone, not in the documentation, nothing else."

The Associated Press found the phone for sale on several major retail websites, offered by an array of companies listed in Shenzhen, in southern China. It could not immediately find a reference to the phone's manufacturer.

G Data said the spyware it found on the N9500 could allow a hacker to steal personal data, place rogue calls, or turn on the phone's camera and microphone. G Data said the stolen information was sent to a server in China.

Read the rest here:
Even Toilets Aren’t Safe as Hackers Target Home Devices

By Amy Thompson, Bloomberg, June 10, 2014

Come home to a hot iron and smoldering clothes this afternoon? Soon, it may not be a sign of forgetfulness, but rather evidence that you’ve been hacked.

In coming years, your smartphone will be able to lock your house, turn on the air conditioning, check whether the milk is out of date, or even heat up your iron. Great news, except that all that convenience could also let criminals open your doors, spy on your family or drive your connected car to their lair.

“As these technologies become more sophisticated, it opens up a broader spectrum of threats,” said Gunter Ollmann, chief technology officer of IOActive, a tech security firm in Seattle. A world of connected devices makes it possible “for the bad guys to have permanent entry into your household.”

What the industry calls “the Internet of things” has been heralded as the next wave of tech riches. By 2020, some 26 billion such devices may be connected to the Internet, up from 3 billion today, researcher Gartner Inc. (IT) estimates. That’s almost four times the number of smartphones, tablets and PCs that will be in use.

The vision is to connect almost everything -- from cars to fridges, lamps, even toilets. Forget to flush? There’s an app for that.

Problem is, data security isn’t typically a big focus for toilet, refrigerator or baby monitor manufacturers. Security lapses on such devices could allow bad guys to disrupt home life, gather valuable personal data, or even use stolen information to extort money from victims, Ollmann said.

Hijacked Robotoilet

Trustwave, a Chicago company that helps corporate clients fight cybercrime, hijacked a Bluetooth connection that controls toilets made by Japan’s Lixil Group. (5938) That could allow hackers to open or close the lid and even squirt a stream of water at the user’s behind, Trustwave said.

Lixil said it’s difficult to commandeer its toilets as hackers would need to connect their smartphone to the loo using a special remote that comes with the device, making abuse “a very rare case.”

Even some tech companies have created devices lacking sufficient protection. Ollmann’s group broke into a home automation system from Belkin International Inc., a company that makes mobile phone accessories and Wi-Fi routers. Belkin’s WeMo box fits over electrical outlets to control lamps, fans, coffee makers and other appliances via a smartphone app.

Fire Hazard

IOActive found a way to take over those switches, turning them into poltergeists that could turn on heaters and irons -- a fire hazard and electricity-waster. Belkin said it discovered the vulnerabilities and fixed them even before IOActive discovered them in an older device.

As home automation technologies spread, appliance makers must educate buyers on security, said John Yeo, a director atSpiderlabs, Trustwave’s research unit. That would include stressing the importance of changing default passwords on such devices, which can allow even relatively unskilled hackers to gain access.

“This push to make everything under the sun Internet connected, perhaps because it’s in many respects aimed at the consumer end of the market, hasn’t had much of a focus on security,” Yeo said.

Companies that produce the next generation of smart appliances aren’t saying much about the topic. Samsung Electronics Co. (005930), which makes washers that users can monitor from their smartphones, said in an e-mail that it “takes the security of its products very seriously” and monitors risks. The company declined to comment further.

Interactive Countertop

LG Electronics Inc. (066570) has Smart ThinQ technology that lets smartphone users monitor and diagnose problems in washers, refrigerators and ovens. The applications require buyers to create a username and password. LG declined to comment.

Sweden’s Electrolux SA is developing an interactive countertop, a white surface with hidden elements for cooking food and charging devices such as mobile phones without plugging them in. The countertop even comes with a virtual chef to walk you through recipes. The company declined to make an executive available for this article.

Though not many criminal hackers are targeting such devices today, that will change once there’s a reliable way to make money from exploiting them, said Sebastian Zimmerman, a member of the Chaos Computer Club, a German hacker collective campaigning to raise awareness of security and privacy.

Read the rest here:
Experts Reveal Police Hacking Methods

By Raphael Satter, Associated Press, June 24, 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.

Drawing on a cache of leaked documents and months of forensic work, two reports about the private Italian firm Hacking Team expose a global network of malicious software implants operated by police and spy agencies in dozens of countries. They also suggest that the lines between high-tech police work and malicious hacking are blurring.

"In the past, the distinction was pretty easy: If it's malware, there's someone bad behind it," said Costin Raiu, a senior security researcher at Russian anti-virus firm Kaspersky. "The notion of good guys and bad guys is becoming diluted."

The reports by Kaspersky and the Toronto-based Citizen Lab help complete the picture of state-sanctioned surveillance sketched by Edward Snowden's sensational revelations about the National Security Agency and its international allies.

While many of Snowden's revelations dealt with the mass monitoring of communication as it flows across the globe, Hacking Team brags about more aggressive forms of monitoring that let authorities turn people's phones and laptops into eavesdropping tools.

Hacking Team, based in Milan, did not return several messages seeking comment.

On its website, the company takes pains to present itself as one of the good guys. In a moody promotional video with a gravelly voice-over, it boasts of being able to steal text messages, eavesdrop on Skype calls and take control of hundreds of thousands of targeted devices at a time.

Hacking Team's customer policy says it sells only to governments, which it screens for human rights concerns. A company-established panel of technical experts and legal advisers checks out every potential client, Hacking Team says, and while it realizes that its software can be abused, "we take a number of precautions to limit the potential for that abuse."

Those precautions haven't prevented copies of Hacking Team's malicious software from being used to target more than 30 activists and journalists, according to a tally maintained by Citizen Lab, a research group based at the University of Toronto's Munk School of Global Affairs.

Citizen Lab's report provided an unusual level of insight into how the malware operates, showing how devices can be compromised through booby-trapped emails or infected USB sticks, or even pushed onto handsets by a pliant telephone company.

Screenshots released by Citizen Lab appear to show a control panel complete with on-off switches for recording text messages, calls, keystrokes and visited websites. Other options open to Hacking Team's customers include the ability to force infected phones to take regular pictures or video and to monitor the position of an infected handset via Google Maps, effectively turning a target's phone into both a hidden camera and a tracking device.

Hacking Team built its programs for stealth. The spy software implanted on iPhones is calibrated to avoid draining the phone's battery, both Citizen Lab and Kaspersky said. On BlackBerrys, it can be programmed to ship stolen data via Wi-Fi to avoid jacking up the phone bill. The spyware even comes with a special "crisis" mode that will cause it to self-destruct if it's in danger of being detected.

"The victim's got almost no chances of figuring out that their iPhone is infected," Kaspersky malware expert Sergey Golovanov said in an interview.

Hacking Team does not say who its customers are, but researchers can draw inferences from the network of servers tasked with controlling its spyware.

In its report, Kaspersky says its scans uncovered 326 Hacking Team command servers based in more than 40 countries, including 64 servers in the United States, 49 in Kazakhstan and 35 in Ecuador. Other countries hosting multiple servers include the United Kingdom, Canada and China.

Read the rest here:
Can digital forensics keep up with smartphone tech?

By William Jackson, GCN, June 16, 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.

“When I started doing forensics, mobile devices meant flip-phones and texting,” said Josh Moulin, a contractor doing forensics work for a federal agency. The information you could expect to get from a phone was a contact list, some text messages and calendar entries.

“Today they are computers, and we are getting everything off of them that we would expect from a computer. You have a great picture of what a person is doing and is interested in.”

But the sheer volume of data and devices can be overwhelming. Forensics labs within law enforcement agencies and in the private sector have backlogs from six to 24 months and are struggling to keep up with the pace of technical change in the devices being examined.

And it’s not just a matter of Android or Apple phones. Forensics professionals estimate there are more than 10,000 models of mobile phones being used today from as many as 3,000 manufacturers. About 150 new phones were released in April alone.

**Inside forensics**

Forensics is the science of developing or extracting information for use in investigations and in civil or criminal court cases. Digital forensics involves getting that information in a digital format, usually from a computer or some form of electronic media. It requires getting access to the device, locating the data, copying it and analyzing it to turn the data into information.

What’s more, if the resulting information is going to stand up in court, each step has to be documented, and care has to be taken not to alter the data being gathered – or the original data.

Digital forensics has been around for decades, but forensics on mobile digital devices is a relatively new and rapidly changing field. Although the two share similarities, “they are very different,” said John Carney, chief technology officer of Carney Forensics, which helps attorneys and investigators glean insights into their cases by retrieving digital forensic evidence.

The most obvious difference is that mobile devices are – well, mobile. “Mobile phones are far more aware of their surroundings,” Carney said. Many have location functions using GPS, which can leave traces on the phone or on applications loaded onto it.

Mobile devices also often have multiple networking options, including cellular, Wi-Fi and Bluetooth, which can keep track of available local networks even if they are not connecting, and providing another picture of where the user has been. The result can be a detailed picture of the owner.

“Mobile phones are a lifestyle,” Carney said, more so than a desktop or laptop computer.

**Investigative hurdles**

However, such connectivity can also pose a threat for investigators – or at the very least block access to devices by forensic analysts. For instance, security tools intended to protect the device can let a remote administrator wipe or lock up a phone remotely. Although this is common in organizations that issue phones to employees, so far it is little used by consumers.

However, the California state senate has passed a bill that would require all smartphones to have a kill switch or shut-off function. The goal is to make the phones less attractive to thieves, but public and private investigators worry that it also could put evidence at risk after a phone has been seized.

To keep a phone from being wiped, locked or otherwise changed after it is seized, investigators now use a Faraday bag, a portable version of the 19th century Faraday cage that uses a mesh of conducting material to block radio signals and static electric fields. Carney isolates phones in a bag using three different metal oxides to block cellular, Wi-Fi and Bluetooth signals.

“Now we actually examine them inside a Faraday bag,” Carney said, by connecting a USB cable to the phone while it is inside the bag to extract data.

Some issues facing forensic analysts are mundane. Keeping track of the USB and other connectors used to access power and data ports on different makes and models of phones is surprisingly difficult.

Read the rest here:
http://gcn.com/articles/2014/06/16/forensics-technology-race.aspx
Report Examines How Attackers Mask Threat Activity

By Mike Lennon, Security Week, June 3, 2014

Smartphone theft is serious business in the US these days and even more worrisome with the BYOD boom in the business world. A new study finds that one in ten smartphone users are victims of device theft, and only 30 percent actually get their stolen smartphones back.

Network security firm Palo Alto Networks has released the latest version of its Application Usage and Threat Report, (http://researchcenter.paloaltonetworks.com/app-usage-risk-report-visualization-2014/) which sheds light on how attackers are exploiting commonly-used business applications to bypass security controls.

According to the report released Monday, common sharing applications such as e-mail, social media, and video remain the attack vehicles of choice for cybercriminals, but are often only the start of multi-phased attacks rather than the focus of threat activity.

“This isn’t really groundbreaking, but we think it’s important for people to understand that threats coming into your network and the data going out of your network are often through completely different means,” Ryan Olson, head of threat intelligence at Palo Alto Networks, told SecurityWeek.

“You really need to have good visibility to tie those together and understand all the applications that are on your network and inspect that traffic,” Olson said.

“Our research shows an inextricable link between commonly-used enterprise applications and cyber threats,” explained Matt Keil, senior research analyst at Palo Alto Networks. “Most significant network breaches start with an application such as e-mail delivering an exploit,” Keil said. “Then, once on the network, attackers use other applications or services to continue their malicious activity – in essence, hiding in plain sight. Knowing how cyber criminals exploit applications will help enterprises make more informed decisions when it comes to protecting their organizations from attacks.”

According to the report, 34 percent of the roughly 2100 applications observed can use SSL encryption. As a result, many network administrators are unaware of what applications on their networks use unpatched versions of OpenSSL, which can leave them exposed to vulnerabilities such as Heartbleed, the security firm warned.

Interestingly, Palo Alto Networks found that 99 percent of all malware logs were generated by a single threat using UDP; attackers also use applications like FTP, RDP, SSL, and NetBIOS to mask their activities.

Read the rest here: http://www.securityweek.com/report-examines-how-attackers-mask-threat-activity

Upcoming Chapter Meetings

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 9</td>
<td>10:45 to 1:00</td>
<td>The Retired Enlisted Association</td>
</tr>
<tr>
<td></td>
<td></td>
<td>834 Emory Circle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(719) 596-0927</td>
</tr>
<tr>
<td>July 17</td>
<td>5:45 to 8:00</td>
<td>TREA</td>
</tr>
<tr>
<td>August 5 &amp; 6</td>
<td>August Cyber Security Training Forum</td>
<td></td>
</tr>
</tbody>
</table>
ISSA meeting photos are courtesy of our Chapter photographer Warren Pearce.

Board members presenting one year memberships to Warren and Paul.
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:

doncream-issa@q.com

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

How Teen Hackers Were Portrayed In 1980s Family Magazines

By Leslie Horn, Gizmodo, June 5, 2014

Like all things, the way we portray hackers in pop culture has evolved through the years. But they were maybe never more adorable than in 1980s family magazines.

According to a USC study that looked at 74 youth- and family-computing publications like FamilyPC and Family Computing from the 80s to show that people didn't see hackers as the enemy, though much of the media did, and a historical precedent was there. Nope, hacker were just clever kids with a penchant for pranks who also happened to like computers:

Read the rest here: http://gizmodo.com/how-teen-hackers-were-portrayed-in-1980s-family-magazin-1586512981