Colleagues,

As I write this we are busily preparing for our Spring conference to be held on 25 March at UCCS. We have several vendors signed up, a very interesting group of speakers focused on cybercrime topics, and a real opportunity to reach out to a population of people working cybersecurity issues in our town who have either never heard of ISSA or don’t fully know the benefits of being a chapter member. This is an opportunity for us all to reach out to our colleagues, customers, and friends who are working in this career field and invite them to a FREE conference where they can earn knowledge, CPEs, and expand their professional network.

I mentioned before we are going to do a professional networking event one evening in April and the board is finalizing the details of what that will look like. If you have ideas of what you would like to see please let your Members-At-Large, Russ Weeks and James Asimah, know. This is something new for us and there are no going-in plans that say ‘we have to do things this way’... let’s make the event something we want it to be, all ideas will receive fair discussion and consideration so bring them up.

One thing that I want our chapter to guard against is keeping things the same for too long. Routines are important and I understand that but a routine chapter can grow stale very quickly. I want a chapter where people show up early to meetings because they are excited to be there or they attend conferences because it

(Continued on page 3)
By Vivek Wadhwa, LinkedIn, April 22, 2013

They don’t prepare you for this in college or admit it in job interviews. The harsh reality is that if you are middle-aged, write computer code for a living, and earn a six-figure salary, you’re headed for the unemployment lines. Your market value declines as you age and it becomes harder and harder to get a job.

I know this post will provoke anger, outrage, and denial. But, sadly, this is the way things are in the tech world. It’s an “up or out” profession — like the military. And it’s as competitive as professional sports. Engineers need to be prepared.

This is not openly discussed, because employers could be accused of age discrimination. But research, such as that completed by University of California, Berkeley, professors Clair Brown and Greg Linden shows that even those with masters degrees and Ph.Ds have reason to worry.

Brown and Linden’s analysis of Bureau of Labor Statistics and Census data for the semiconductor industry revealed that although salaries increased dramatically for engineers in their 30s, these increases slowed after the age of 40. After 50, the mean salary fell by 17% for those with bachelors degrees and by 14% for those with masters degrees and Ph.Ds. And salary increases for holders of postgraduate degrees were always lower than for those with bachelor’s degrees (in other words, even Ph.D degrees didn’t provide long-term job protection).

It’s the same in the software industry. Prominent Silicon Valley investors often talk about youth being an advantage in entrepreneurship. If you look at their investment portfolios, all you see are engineers who are hardly old enough to shave. They rarely invest in people who are old.

It may be wrong, but look at this from the point of view of the employer. Why would any company pay a computer programmer with out-of-date skills a salary of say $150,000, when it can hire a fresh graduate — who has no skills — for around $60,000? Even if it spends a month training the younger worker, the company is still far ahead. The young understand new technologies better than the old do, and are like a clean slate: They will rapidly learn the latest coding methods and techniques, and they don’t carry any “technology baggage.” The older worker likely has a family and needs to leave the office by 6 p.m. The young can easily pull all-nighters.

What the tech industry often forgets is that with age comes wisdom. Older workers are usually better at following direction, mentoring, and leading. They tend to be more pragmatic and loyal, and to know the importance of being team players. And ego and arrogance usually fade with age.

During my tech days, I hired several programmers who were over 50. They were the steadiest performers and stayed with me through the most difficult times.

It can be difficult for some companies to justify paying the age premium. For tech startups in particular, it always boils down to cost: Most can’t even afford to pay $60,000 salaries, so they look for motivated, young software developers who will accept minimum wage in return for equity ownership and the opportunity to build their careers.

We can blame the employer, but in a free economy you can’t really force any company to hire workers who have the wrong skills or to pay higher salaries. Larger companies develop products for global markets and have global workforces. They will hire where they can get the best skill for the best price.

So, whether we like it or not, it’s a tough industry, and the onus is on employees to keep themselves marketable. I know that many people will take offense at what I have to say, but here is my advice to those whose hair is beginning to grey.

Read the rest here:
https://www.linkedin.com/pulse/20130422020049-8451-the-tech-industry-s-darkest-secret-it-s-all-about-age
We participated in Colorado Technical University’s (CTU) networking event during February and spoke to several students potentially interested in joining and participating in the student mentorship program. We will be following up with folks this month. Hopefully we’ll gain some new members. We’ve been trying to expand our reach into other local universities and this appears to have been a good opportunity.

Last month I mentioned that we were looking for part-time job opportunities or internships. Thanks for your responses—we’ve received several openings and have passed them on to our student members. Please keep us in mind and send any of those types of opportunities to Melissa or Dave so we can get them out to our student members.

We received very good feedback on the two new committees—Ethics and Marketing. Gee, that almost sounds like a training topic for the new Ethics committee, but, I digress. J Your responses have filled the Ethics committee and have started filling the Marketing committee. We still need some more volunteers to help out with the Marketing committee so if you’re interested, please contact Suzanne Chance at marketing@issa-cos.org and join the team. As Tim Westland and Suzanne begin to get their respective committees off the ground, I’m sure we’ll be seeing some feedback from them soon.

We seem to be holding our own with numbers, showing a slight increase in our total—we hit 388. So, our renewals and new members are keeping pace with our losses in this transient community. That’s great news and we need to continue our efforts to find new members and remind current members to renew. We are anticipating a response soon from ISSA International on some changes that will allow us to expand our student outreach and sponsorships. Hopefully, we’ll have that in place for next month’s newsletter.

Last, and of course not least, 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.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

(Continued from page 1)

A Note From Our President

really benefits them professionally. If you’re just coming for the CPEs, it’s still great to see you but let me know that because your chapter should be more to you than just a CPE opportunity. Your entire chapter board is very open to hearing from you, write us anytime at cos-board@issa-cos.org or grab us at a meeting and let’s talk about how we can better meet your needs.

Thanks for all you do, hope to see you at the March conference.

Cheers!

Pat
### Chapter Financials

**Courtesy of our Treasurer—Melody Wilson**

<table>
<thead>
<tr>
<th>Account status</th>
<th>3/3/2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Savings</td>
<td>$88.69</td>
</tr>
<tr>
<td>Checking</td>
<td>$7588.10</td>
</tr>
<tr>
<td>Membership checking</td>
<td>$1434.87</td>
</tr>
<tr>
<td>Travel Support checking</td>
<td>$100.00</td>
</tr>
<tr>
<td>Training checking</td>
<td>$93.25</td>
</tr>
<tr>
<td>Cash (change/tips)</td>
<td>$0.00</td>
</tr>
<tr>
<td>PayPal Account</td>
<td>$2,926.63</td>
</tr>
<tr>
<td>Training Bank Account</td>
<td></td>
</tr>
<tr>
<td>Training Petty Cash</td>
<td>========</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>$12,231.54</strong></td>
</tr>
</tbody>
</table>
Training Team Update

Study Groups

Organized study groups are in progress for two certifications. A study group for the CISSP concentration, Information Systems Security Architecture Professional (ISSAP) started 12 Feb and the next meeting is scheduled for 12 Mar, 5:00 – 6:00pm, at the East Library. A study group for the Certified Authorization Professional (CAP) certification is scheduled to start on 5 Mar, 6:00 – 7:30pm, at the East Library. Also, a few members have expressed interest in participating in a study group for the Certified Information Systems Manager (CISM) certification. If you would be willing to organize/facilitate a study group for the CISM, or would like to participate in a CISM study group, please let me know. Additional study groups can be organized for other certifications if there are enough members interested and if someone is willing to take on the role of organizing and scheduling the meetings.

Contact Colleen Murphy (crmurphy.cs@hotmail.com) if you’re interested in organizing a study group, want to participate in a study group, or if you have questions.

Security+

The first Security+ Exam Prep Review Seminar for 2015 is scheduled for 11 April at Colorado Technical University (CTU) (See the ad on page 6.) The cost for this one-day seminar is only $25, so it’s a great way to get certified! Registration information will be sent out by the middle of March. If you already hold the Security+ certification, consider attending a Security+ Exam Prep Review Seminar for an update and for CEUs. Members wishing to attend for CEUs still need to register, and may be limited to space-available only.

Contact Colleen Murphy (crmurphy.cs@hotmail.com) to register for the seminar, to volunteer as a Security+ instructor, or if you have questions.

We have a lot planned for this year, so stay tuned for updates.

A Note from Our Vice President

Just want to say a quick thank you to all the members that helped during the February Dinner and the event at CTU. I really appreciate the help.

If there is anyone who like to help with the March conference please contact me at thornbuc@aol.com. I currently have 4 people who have volunteered to help. We need more volunteers for the sign-in desk, work the ISSA table, POC for the vendors (answer questions), POC for speakers (make sure their slides are set up and answer questions) and help with the break out rooms.

Cindy
The Colorado Springs Chapter of ISSA is hosting an 8-Hour Security+ Exam Preparation Seminar

Location: Colorado Technical University (CTU) Room 102
4435 N. Chestnut St., Colorado Springs, CO 80907

Date: 11 Apr 2015

Time: Check in between 8:00 AM – 8:15 AM
Class starts at 8:15 AM and runs to 4:45 PM (30 min lunch)

Cost: $25.00 (includes refreshments)

REGISTRATION & VOLUNTEER INSTRUCTORS CONTACT:

Register for class via: http://eventbrite.com, or provide your name and contact info to Colleen Murphy at: crmurphy.cs@hotmail.com. Questions; please call Colleen at: 719-651-0415.

UPDATED COURSE CONTENT AND IN-CHAPTER INSTRUCTORS

- Updated and expanded material - Test Objectives & Exam Tips
- Full day program with one session for each of the six domains
- Each block of instruction covers one exam objective
- All Instructors are Security+ Certified

TOPICS COVERED INCLUDE:

- Network Security
- Compliance and Operational Security
- Threats and Vulnerabilities
- Application, Data, and Host Security
- Access Control and Identity Management
- Cryptography

TO BECOME A MEMBER OF ISSA visit: www.issa.org/Join ISSA. Specify the Colorado Springs Chapter.
Are You a Risk to Your Own Firm or Business?

By David Willson, ISSA-COS, February 28, 2015

An extensive and sophisticated cyber espionage operation targeting mainly Western military, government, defense industry firms, and the media, now has a new weapon: a spyware app for Apple iPhones and iPads.

Despite all of the bad news and negativity in the world, most of us have a very positive or even inflated opinion of ourselves. How many people believe they are ugly, bad drivers, or disliked by others? Very few. As the owner or partner of a law firm or business-owner, you may be one of the greatest risks to your own organization. Many successful business leaders are type-A personality, extremely sure of themselves and believe their manner of doing business is better than the next guy or gal. In business this is exactly what is needed, and that is why many are so successful. But, when it comes to cyber-security this attitude creates a blind side to the realities of how vulnerable we really are.

This article discusses four factors impacting law firm owners/partners and business owners that may significantly increase cyber risk, and thus potential liability, loss of business and reputation:

“Optimism bias” and complacency;

“Convenience v. security”;

The “emperor has no clothes” syndrome; and,

Self-imposed ignorance.

First, it’s safe to say, and hopefully all will agree, cyber-security, data breaches and hacking, have become a very big deal. If you have not heard about the data breaches at Target, Home Depot, NSA, the Pentagon, Lockheed-Martin, the local Liquor store? Remember the movie, My Cousin Vinny? Joe Pesci, who plays Vinny Gambini, is defending his nephew and his nephew’s friend who are accused of robbing a convenience store and murdering the clerk. Vinny is questioning a witness to the crime who states that when he began to make his breakfast, eggs and grits, he saw the defendants go into the convenience store. The witness then testifies that 5 minutes later he sees the two boys leave the store when he is about to eat his breakfast:

“Vinny Gambini: So, Mr. Tipton, how could it take you five minutes to cook your grits, when it takes the entire grit-eating world twenty minutes?

Mr. Tipton: [a bit panicky] I don't know. I'm a fast cook, I guess.

Vinny Gambini: I'm sorry; I was all the way over here. I couldn't hear you. Did you say you were a fast cook? That's it?

[Mr. Tipton nods in embarrassment]

Vinny Gambini: Are we to believe that boiling water soaks into a grit faster in your kitchen than on any place on the face of the earth?

Mr. Tipton: I don't know.”

Ask yourself, “Do the standard security practices work better on your network, or do you use magic security

(Continued on page 8)
practices no one else is aware of?" Whether you are the victim of a random drive-by breach or specifically attacked like the law firms targeted by China in order to gain mergers and acquisition data on their clients, you are under attack and you will likely fair no better than most, certainly the big guys.6

So, what may cause us to believe our security is better? This attitude can blind us to reality, especially because it leads us to become complacent and not concern ourselves with security. As stated above, most of those surveyed believe their security is pretty good, certainly better than their neighbor’s, and the chances of suffering a breach are fairly low. In reality most firms/businesses either will be or have already been breached.7 Amazingly, most business owners who claim they won’t be breached also had little to do with the implementation of their own security and likely do not really understand it.

Passively assuming someone else, like your outsourced IT Company or your in-house IT department, is identifying and addressing the threats and risks is not an adequate form of risk management. Even if your firm/business has or uses a CFO aren’t you familiar with and understand the finances and budget of your firm/business? To ignore this would be dangerous and potentially negligent. So, why do we ignore our security? We need to get better acquainted with the security currently employed and identify potential risks. As the lawsuits mount after the above-mentioned recent high profile breaches and CEO’s are fired or resign, you can no longer take a hands-off complacent attitude when it comes to technology, cyber-security and risk.

The next factor is what I refer to as “convenience v. security.” Technology has been both a blessing and a curse. Most of us have a love-hate relationship with our computers and mobile devices. Very rarely do you hear people say, “I love my smart phone or iPad, or whatever device,” but, we can’t live without them. In fact, some people are so obsessed that they are willing to camp out in front of the store for days to be the first to get the latest and greatest device. What we love about them is the convenience and security threatens that convenience. Most people find the security practices tiresome, awkward, and annoying. For instance, do you password protect your smartphone or mobile device? Passwords are annoying though, right? So, a lot of people either don’t use one or use a very easy password, like 1234. In 2014 3.1 million smartphones were stolen.8 The number lost is probably at least equal to or greater than that. What would a thief or someone who found your smartphone or mobile device have access to if it was stolen or lost? Do you have to log into your social media on your mobile device or can you login automatically? If automatically then that person now has access to all of your social media, email, texts, contacts, etc. But, we find the security rules for our devices inconvenient and so either ignore them or attempt to make them as simple as possible or find a workaround. As Job stated, “Shall we indeed accept good from God, and shall we not accept adversity?”9 Shall we accept the convenience of technology and ignore the risks? Think about the volumes of data that your firm deals with, creates, receives, transmits, and carries around monthly. It is all at risk. Are you willing to increase that risk because you find security rules inconvenient?

The third factor is called the “emperor has no clothes” syndrome. The job of securing the network, all mobile devices, and anything else related to technology and the information that flows across it has fallen in the laps of the IT Company or department. Granted, many firms or businesses have hired CISOs (chief information security officers) and other experts, but the majority of businesses and law firms have not. Some IT professionals may be skilled and thus able to serve a dual-role as security and IT professionals, but most are not. So, the battle begins. That is, the battle for budget. Now, if you are the IT guy, your primary focus is likely “uptime” and making sure everyone can access the network. Security, unfortunately, plays second fiddle, and revealing how vulnerable the network is may not bode well if the boss is constantly hearing the negative. In some cases the IT department or company doesn’t know the full risk or extent of the vulnerabilities, but this is unlikely. What is more likely is that they know but are hesitant to reveal how bad it really is, how vulnerable you really are, for fear of the impression it will create, e.g. maybe they are not able to fully secure the network or are just looking for more money. Regardless of the reason or reasons, the message about how much risk exists gets lost and never conveyed to leadership. This is a risk in and of itself. IT departments and companies are playing with fire if they don’t reveal the true risks and vulnerabilities and allow the leaders to address them. Have you have seen some of the TV ads for anti-virus companies that claim to speed up and protect your computer? Whether their contract says it or not, many of them are making it appear that they will make you 100% secure. Well, they aren’t and they can’t. If you purchase their product and then get a nasty virus and lose some or all of your data you will be pretty mad and likely consider suing. Owners, partners, managers, leaders, if you are given the impression your network is secure, or not told about how vulnerable it is and therefore assume it is secure, will your reaction be when you are breached? Likely, what the “#$&? IT departments and companies, tell the truth, the whole truth and nothing but the truth, they need to know. Owners, partners, managers, leaders or bosses, you need to know how bad it is in order to evaluate and mitigate the risks, so go ask.

The final factor is self-imposed ignorance, which comes with a downplaying of the threat, maybe some “optimism bias,” and, as mentioned above, ignorance of the seriousness of the risks facing the firm or business. When I speak to companies about cyber-security and the need for a risk assessment, I hear far too often: “I’m not worried, I don’t have anything the hackers want to steal;” “I’m not worried, my business is too small;” or, “I’m not worried, our IT guys make us use really good passwords and we have cyber insurance.” Wow! That’s like saying; “I will never get in a car accident because I am a great driver.” Some things you just can’t control. There is an old saying that goes: “There are two things you can count on,
Request for Chapter Presenters

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
Join us for the 2nd Annual Information Systems Security Association (ISSA) - Colorado Springs Chapter - Cyber Focus Day (www.fbcinc.com/cfd) set to take on Wednesday, March 25, 2015 at the University of Colorado - Colorado Springs (UCCS).

Subject matter experts will be on hand to brief attendees on the latest trends, best practices, and remediation strategies in cybersecurity and cybercrime. This one-day forum will offer cyber, IT, business, law enforcement, government, military, academic, training, and other professionals a unique, local opportunity to get up-to-date information on rapidly evolving cybersecurity challenges.

This will also be an excellent opportunity to network with peers, and to join the cybersecurity conversation in Colorado Springs.

**NO COST TO ATTEND:**
Attendance for ISSA members, military/government personnel, and contractors (with a .gov or .mil e-mail address) is free. *CPE/CEU Certificates will be available for attendees.

**EXHIBIT, SPONSOR OR SPEAK:**
Presentation sessions are still available and you can showcase your company’s capabilities as an exhibitor/sponsor. For more information contact Dennis O’Neill at dennis@fbcinc.com.

Hosted by the Information Systems Security Association – Colorado Springs Chapter: www.issa-soc.org
death and taxes.” I would add a third, getting hacked! It will happen. In fact it probably already has and you don’t even know it.

There are many tips, procedures and techniques you can implement to improve your security, but, in my opinion, the first place to start and most important is to do a self-risk assessment:

- Understand the information you collect;
- How it flows across your network;
- What devices it resides on;
- Who has access to it;
- How it is kept secure, and;
- Who you are connected to, (e.g. ISP, Cloud provider, other services, etc.).

If an incident occurs or a client asks what you did or are doing to secure data, responding with, “I don’t know, ask my IT guy,” or, “We use really good passwords,” is not sufficient and will significantly increase your liability and make you look incompetent about an issue that is foremost on most people’s minds these days.

The point is, take an active role. You need to lead and manage the process. Don’t just hand it over to someone else like the IT department or an IT guy or company, and forget about it. Never assume your security is great, good or even adequate. It’s not. Security is not a set and forget concept but a process. Manage it. At any given time you must be able to articulate what you have done to protect data and the firm or business. Pointing to the IT guy or someone else is not a risk management solution or a valid response during an incident response investigation. Are you a basic, progressing or advanced organization?

Take charge, take control, and manage.

David Willson is a retired Army JAG. Among his assignments he worked at NSA and helped to establish CYBERCOM and provided legal advice many cyber operations and policy. He is owner of Titan Info Security Group and is licensed in CO, NY and CT. He specializes in risk management and cyber security helping companies and law firms lower the risk of a cyber incident and reducing the potential liability if and when the firm or its vendor is compromised and all of the client information is stolen. He also provide cyber security awareness training and assists with other unique cyber issues related to discovery, evidence, trial prep, forensics and more. His website is at www.titaninfosecuritygroup.com and he can be contacted at 719-648-4176, or david@titaninfosecuritygroup.com.

ENDNOTES:

5. IMDb, “My Cousin Vinny Quotes.”
7. Cowley, Stacey, “FBI Director: Cybercrime will eclipse terrorism,” CNNMoney, quoting Robert Mueller, Director of the FBI, speaking at the 2012 RSA Conference: “There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again, . . . .”
8. “Smart phone thefts rose to 3.1 million last year, Consumer Reports finds,” ConsumerReports.org, May 2014.
How the NSA’s Firmware Hacking Works and Why It’s So Unsettling

By Kim Zetter, Wired, February 22, 2014

One of the most shocking parts of the recently discovered spying network Equation Group is its mysterious module designed to reprogram or reflash a computer hard drive’s firmware with malicious code. The Kaspersky researchers who uncovered this said its ability to subvert hard drive firmware—the guts of any computer—“surpasses anything else” they had ever seen.

The hacking tool, believed to be a product of the NSA, is significant because subverting the firmware gives the attackers God-like control of the system in a way that is stealthy and persistent even through software updates. The module, named “nls_933w.dll”, is the first of its kind found in the wild and is used with both the EquationDrug and GrayFish spy platforms Kaspersky uncovered.

It also has another capability: to create invisible storage space on the hard drive to hide data stolen from the system so the attackers can retrieve it later. This lets spies like the Equation Group bypass disk encryption by secreting documents they want to seize in areas that don’t get encrypted.

Kaspersky has so far uncovered 500 victims of the Equation Group, but only five of these had the firmware-flashing module on their systems. The flasher module is likely reserved for significant systems that present special surveillance challenges. Costin Raiu, director of Kaspersky’s Global Research and Analysis Team, believes these are high-value computers that are not connected to the internet and are protected with disk encryption.

Here’s what we know about the firmware-flashing module.

How It Works

Hard drive disks have a controller, essentially a mini-computer, that includes a memory chip or flash ROM where the firmware code for operating the hard drive resides.

When a machine is infected with EquationDrug or GrayFish, the firmware flasher module gets deposited onto the system and reaches out to a command server to obtain payload code that it then flashes to the firmware, replacing the existing firmware with a malicious one. The researchers uncovered two versions of the flasher module: one that appears to have been compiled in 2010 and is used with EquationDrug and one with a 2013 compilation date that is used with GrayFish.

The Trojanized firmware lets attackers stay on the system even through software updates. If a victim, thinking his or her computer is infected, wipes the computer’s operating system and reinstalls it to eliminate any malicious code, the malicious firmware code remains untouched. It can then reach out to the command server to restore all of the other malicious components that got wiped from the system.

Even if the firmware itself is updated with a new vendor release, the malicious firmware code may still persist because some firmware updates replace only parts of the firmware, meaning the malicious portions may not get overwritten with the update. The only solution for victims is to trash their hard drive and start over with a new one.

The attack works because firmware was never designed with security in mind. Hard disk makers don’t cryptographically sign the firmware they install on drives the way software vendors do. Nor do hard drive disk designs have authentication built in to check for signed firmware. This makes it possible for someone to change the firmware. And firmware is the perfect place to conceal malware because antivirus scanners don’t examine it. There’s also no easy way for users to read the firmware and manually check if it’s been altered.

The firmware flasher module can reprogram the firmware of more than a dozen different hard drive brands, including IBM, Seagate, Western Digital, and Toshiba.

“You know how much effort it takes to land just one firmware for a hard drive? You need to know specifications, the CPU, the architecture of the firmware, how it works,” Raiu says. The Kaspersky researchers have called it “an astonishing technical accomplishment and is testament to the group’s abilities.”

Read the rest here:
http://www.wired.com/2015/02/nsa-firmware-hacking/
Surprise! America Already Has a Manhattan Project for Developing Cyber Attacks

By Kevin Poulson, Wired, February 18, 2015

“What we really need is a Manhattan Project for cybersecurity.” It’s a sentiment that swells up every few years in the wake of some huge computer intrusion—most recently the Sony and Anthem hacks. The invocation of the legendary program that spawned the atomic bomb is telling. The Manhattan Project is America’s go-to shorthand for our deep conviction that if we gather the smartest scientists together and give them billions of dollars and a sense of urgency, we can achieve what otherwise would be impossible.

A Google search on “cyber Manhattan Project” brings up results from as far back as 1997—it’s second only to “electronic Pearl Harbor” in computer-themed World War II allusions. In a much-circulated post on Medium last month, futurist Marc Goodman sets out what such a project would accomplish. “This Manhattan Project would help generate the associated tools we need to protect ourselves, including more robust, secure, and privacy-enhanced operating systems,” Goodman writes. “Through its research, it would also design and produce software and hardware that were self-healing and vastly more resistant to attack and resilient to failure than anything available today.”

These arguments have so far not swayed a sitting American president. Sure, President Obama mentioned cybersecurity at the State of the Union, but his proposal not only doesn’t boost security research and development, it potentially criminalizes it. At the White House’s cybersecurity summit last week, Obama told Silicon Valley bigwigs that he understood the hacking problem well—“We all know what we need to do. We have to build stronger defenses and disrupt more attacks”—but his prescription this time was a tepid executive order aimed at improving information sharing between the government and industry. Those hoping for something more Rooseveltian must have been disappointed.

On Monday, we finally learned the truth of it. America already has a computer security Manhattan Project. We’ve had it since at least 2001. Like the original, America’s cyber Manhattan Project is purely offensive.

This revelation came by way of the Russia-based antivirus company Kaspersky. At a conference in Cancun this week, Kaspersky researchers detailed the activities of a computer espionage outfit it calls the “Equation Group,” which, we can fairly surmise from previous leaks, is actually the NSA’s Tailored Access Operations unit. NSA’s cyber capabilities have been broadly known since the German news magazine Der Spiegel published a leaked 50-page catalog of NSA spy gear and malware in late 2013. But the one-page catalog descriptions didn’t convey the full flavor of the NSA’s technology. For that, somebody had to actually get their hands on that technology—capture it in the wild—and take it apart piece by piece, which is what Kaspersky did.

The result is impressive. The company has linked six different families of malware—“implants,” as the NSA calls them—to the Equation Group, the oldest of which has been kicking around since 2001. The malware has stayed below the radar in part because the NSA deploys it in limited, cautious stages. In the first stage, the agency might compromise a web forum or an ad network and use it to serve a simple “validator” backdoor to potential targets. That validator checks every newly infected computer to see if it’s of interest to the NSA. If not, it quietly removes itself, and nobody is the wiser.

Only if the computer is a target of interest to the NSA does the validator take the next step and load a more sophisticated implant from a stealth NSA website like suddenplot.com or technicalconsumerreports.com. That’s where it gets interesting. The top tier of NSA malware discovered by Kaspersky is a generation ahead of anything previously reported in the wild. It uses a well-engineered piece of software called a bootkit to control the operating system from the ground up. It hides itself encrypted in the Windows registry, so that anti-virus software can’t find it on the computer’s disk. It carves out its own virtual file system on your machine to store data for exfiltration.

Read the rest here:
http://www.forensicmag.com/articles/2015/01/obama-cybersecurity?type=headline
SSL-busting code that threatened Lenovo users found in a dozen more apps

"What all these applications have in common is that they make people less secure."

By Dan Goodin, ArsTechnica, February 22, 2015

The list of software known to use the same HTTPS-breaking technology recently found preinstalled on Lenovo laptops has risen dramatically with the discovery of at least 12 new titles, including one that's categorized as a malicious trojan by a major antivirus provider.

Trojan.Nurjax, a malicious program Symantec discovered in December, hijacks the Web browsers of compromised computers and may download additional threats. According to a blog post published Friday by a security researcher from Facebook, Nurjax is one such example of newly found software that incorporates HTTPS-defeating code from an Israeli company called Komodia. Combined with the Superfish ad-injecting software preinstalled on some Lenovo computers and three additional applications that came to light shortly after that revelation, there are now 14 known apps that use Komodia technology.

"What all these applications have in common is that they make people less secure through their use of an easily obtained root CA [certificate authority], they provide little information about the risks of the technology, and in some cases they are difficult to remove," Matt Richard, a threats researcher on the Facebook security team, wrote in Friday's post. "Furthermore, it is likely that these intercepting SSL proxies won't keep up with the HTTPS features in browsers (e.g., certificate pinning and forward secrecy), meaning they could potentially expose private data to network attackers. Some of these deficiencies can be detected by antivirus products as malware or adware, though from our research, detection successes are sporadic."

Komodia, a company that brazenly calls one of its software development kits as an "SSL hijacker," is able to bypass secure sockets layer protections by modifying the network stack of computers that run its underlying code. Specifically, Komodia installs a self-signed root CA certificate that allows the library to intercept encrypted connections from any HTTPS-protected website on the Internet. This behavior is by no means unique to Komodia, Superfish, or the other programs that use the SSL-breaking certificates. Antivirus apps and other security-related wares often install similar root certificates. What sets Komodia apart from so many others is its reuse of the same digital certificate across many different computers.

Researchers have already documented that the password protecting most or all of the Komodia certificates is none other than "komodia". It took Errata Security CEO and whitehat hacker Rob Graham only three hours to crack this woefully weak password. From there, he used the underlying private key in the Komodia certificate to create fake HTTPS-enabled websites for Bank of America and Google that were fully trusted by Lenovo computers. Despite the seriousness of Graham's discovery and the ease other security researchers had in reproducing his results, Superfish CEO Adi Pinhas issued a statement on Friday saying Superfish software posed no security risk.

According to Facebook's Richard, more than a dozen software applications other than Superfish use Komodia code. Besides Trojan.Nurjax, the programs named included:

- CartCrunch Israel LTD
- WiredTools LTD
- Say Media Group LTD
- Over the Rainbow Tech
- System Alerts
- ArcadeGiant
- Objectify Media Inc
- Catalytix Web Services
- OptimizerMonitor

A security researcher who goes by the Twitter handle @TheWack0lian said an additional piece of software known as SecureTeen also installed Komodia-enabled certificates. Over the weekend, the researcher also published findings documenting rootkit technology in Komodia code that allows it to remain hidden from key operating system functions.

Read the rest here:
http://arstechnica.com/security/2015/02/ssl-busting-code-that-threatened-lenovo-users-found-in-a-dozen-more-apps/
More than two years after his arrest, Russian national Vladimir Drinkman, 34, who's been charged with masterminding the biggest hack attack in U.S. history, has finally been extradited to the United States. He appeared in a New Jersey federal courtroom Feb. 17, where he pleaded not guilty to 11 charges filed against him by the U.S. Department of Justice.

Drinkman was arrested by Dutch authorities on June 28, 2012, at the request of U.S. prosecutors. But he remained incarcerated in the Netherlands while the Dutch government reviewed competing extradition requests that were filed by U.S. and Russian authorities. In November 2014, however, Dutch Justice and Security Minister Ivo Opstelten upheld the U.S. extradition request for Drinkman on the grounds that U.S. authorities filed their request first.

U.S. authorities have hailed the extradition as a model of transnational cooperation. "Hackers often take advantage of international borders and differences in legal systems, hoping to evade extradition to face justice," says U.S. Assistant Attorney General Leslie Caldwell. "This case and today's extradition demonstrates that through international cooperation, and through great teamwork between the Department of Justice and the Department of Homeland Security, we are able to bring cyber thieves to justice in the United States, wherever they may commit their crimes."

Drinkman allegedly ran a group that included three other Russians and one Ukrainian who were indicted in 2013 over their alleged involvement in a credit and debit card fraud scheme that resulted in more than 160 million cards being stolen from payments processors Global Payments and Heartland Payment Systems, as well as grocery chain Hannaford Brothers, among other organizations, according to a second superseding indictment, which was unsealed in July 2013 in Newark federal court.

Between 2005 and 2012, according to the indictment, Drinkman's gang allegedly launched attacks against NASDAQ, 7-Eleven, Carrefour, JCP, Hannaford, Heartland, Wet Seal, Commidea, Dexia, JetBlue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard. U.S. authorities say that NASDAQ's trading platform was not affected by those attacks. They also note that the fraud losses incurred by just three of the hacked organizations topped $300 million.

Five Men Charged

Drinkman's cybercrime ring often hacked into websites by exploiting SQL injection flaws, court documents allege. But according to the indictment, the alleged members of the hacking team brought different skills to bear:

- Drinkman is a "sophisticated hacker" and expert at "penetrating network security and gaining access to the corporate victims' systems," the indictment says;
- Alexandr Kalinin, 28, is described as having the same skills as Drinkman, and has been charged in two other federal indictments with hacking NASDAQ, as well as multiple U.S. financial institutions;
- Roman Kotov, 33, "specialized in mining the networks Drinkman and Kalinin compromised to steal valuable data";
- Mikhail Rytikov, 27, provided "anonymous web-hosting services" used by attackers. He's also been charged for an unrelated attack;
- Dmitriy Smilianets, 31, "sold the information stolen by the other conspirators and distributed the proceeds of the scheme to the participants."

Both Drinkman and Kalinin were previously charged in a 2009 indictment that tied Albert Gonzalez to five corporate hacking campaigns, including the Heartland data breach, which at the time was the biggest-ever reported breach. Gonzalez perpetrated those attacks at the same time as he was helping U.S. authorities investigate the notorious global cybercrime ring known as "Shadowcrew." Gonzalez is serving a 20-year prison sentence.

Read the rest here:
http://www.govinfosecurity.com/alleged-russian-mega-hacker-extradited-a-7928
Chapter Activity in February
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...

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

What the NY Times thought about the laptop 30 years ago


The limitations come from what people actually do with computers, as opposed to what the marketers expect them to do. On the whole, people don't want to lug a computer with them to the beach or on a train to while away hours they would rather spend reading the sports or business section of the newspaper. Somehow, the microcomputer industry has assumed that everyone would love to have a keyboard grafted on as an extension of their fingers. It just is not so.

The proponents of portables stoutly maintain that the stumbling block to a computer in every attaché case is price. Right now, a laptop computer costs considerably more than the equivalent desktop version.

Read the rest here: