We Need to Disrupt Cybercrime

Law enforcement agencies lack the resources to prosecute all cybercrime. Instead they will need disrupt it, says Europol's Troels Oerting.

By InfoSecurity Magazine, April 20, 2014

Law enforcement agencies will no longer have the resources to investigate, or prosecute, all cybercrime. That was the stark warning given by Europol's Troels Oerting, during his opening keynote at Infosecurity Europe 2014.

Instead, agencies need to put more emphasis on disrupting cybercrime. This may mean not investigating some crimes, and accepting a degree of loss. Police force cybercrime units, and other investigators, will be forced to prioritise. "There may be crimes we don't investigate," he said.

The warning comes against a background of growing internet use, and a growing dependence on the internet, in Europe.

According to Oerting, 78% of Europeans are now online, and economies depend on the net for their operations. "In a physical attack there is a link between the perpetrator and the crime scene, and you can profile the criminals," Oerting told the Infosecurity Europe audience. "But that is not the case with cybercrime."

Cybercrime is becoming increasingly organised and

Due to unforeseen circumstances there will not be "A Note From Our President this month."

But a move away from manufacturing, to knowledge-based industries, has opened up new avenues for crime.

Oerting pointed out that law enforcement officers divide criminality into two categories: cybercrime, and internet "assisted" crime. Assisted cybercrime includes activities such as financial fraud and theft from banks' ATMs, as well as child abuse images.

Criminals are using the net, and especially the dark net, to communicate, collaborate and sell their wares; they send funds using Bitcoin. It is becoming harder to "follow the money", and even agencies such as the NSA struggle to see inside the dark net, he said.

Cybercrime, for its part, is borderless and leaves little in the way of a physical evidence trail. "In a physical attack there is a link between the perpetrator and the crime scene, and you can profile the criminals," Oerting told the Infosecurity Europe audience. "But that is not the case with cybercrime."

Cybercrime is becoming increasingly organised and (Continued on page 3)
By UC Irvine, April 16, 2014
In 2000, 15-year-old Jonathan Lebed made headlines – and financial history, of sorts – when he became the first minor ever charged with stock market fraud by the U.S. Securities & Exchange Commission.

According to the SEC, the New Jersey teen used his computer to execute a classic pump-and-dump scheme. He snapped up cheap penny stocks, spread false rumors about them on financial message boards under various aliases, and then sold them for a tidy profit. His investments, ranging from an importer of Italian cheese to a manufacturer of bendable toy figures, netted him hundreds of thousands of dollars – as much as $74,000 in a single day. The SEC dropped the charges against Lebed after he agreed to hand over $285,000 in ill-gotten gains.

Shady stock trades are nothing new to Henry Pontell, UC Irvine professor of criminology, law & society and sociology. An expert on white-collar crime, he’s studied Wall Street rip-offs and other forms of financial fraud for three decades, even testifying on the subject before the U.S. Senate in 2010. What’s changed isn’t the scam but the artist: In this digital age, the criminal mastermind is often a mere child.

It’s something Pontell hadn’t seen before the widespread use of the Internet. Elaborate stock swindles, identity thefts and other big-money heists have been orchestrated online by adolescents, some not even old enough to drive. The perps have pimples.

“Fifteen seems to be the magic number. I don’t know why. It’s something about hormones or not getting dates,” Pontell says, half-jokingly. “They’re not really grownups and not really kids, and they probably aren’t dating a lot. They’re stuck in their rooms with their computers. That plays into this. They’re at the peak of their techno-geekiness. And they’re really savvy.”

One of the first in his field to study cybercrime, Pontell once summed up the threat such “geeks” pose this way: “There are kids out there today who can steal your identity, destroy your credit and empty out your bank account without ever leaving their computers. And they can do it as fast as unwrapping their birthday presents.”

In the 2010 edition of Profit Without Honor: White-Collar Crime and the Looting of America, an academic text he wrote with Stephen Rosoff and Robert Tillman, Pontell added research on Lebed and other juvenile cybercriminals.

Cases in which adolescents pull off sophisticated swindles are such a new form of deviance that he and Rosoff invented a term for it: white-collar delinquency.

In a 2008 study, Pontell and Rosoff reported that 24 percent of those charged under the federal Computer Fraud and Abuse Act between March 1998 and July 2005 were under age 20. The median financial loss was $59,000 per case – making kids’ weekly allowance look like chump change. Before the Internet, one had to at least pass for an adult to score that kind of money.

“You had to do all kinds of physical things to commit a white-collar crime,” Pontell notes. “A 15-year-old can’t pose as a stockbroker.”

Underage cybercriminals don’t fit the traditional profile of juvenile delinquents, he says. They’re not the typical troublemakers, the ones already on law enforcement’s radar for truancy, drug use and gang behavior.

Among middle and high school students, those most likely to engage in illegal online acts had friends who did so, according to a 2011 study led by Michigan State University criminologist Thomas Holt. Other determining factors included the amount of time they spent on computers for nonacademic reasons, lack of self-control and having strong tech skills. Higher grades were not an indicator, and girls were highly unlikely to commit cybercrimes.

“It’s a male-dominated activity,” Pontell says.

To his classmates, coaches and friends, Cole Bartiromo appeared to be an ordinary high school student involved in the usual extracurricular activities: playing baseball, working at a local pizza joint and trading sports cards. But that wasn’t all he traded.

Read the rest here:
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 much 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.

So far I’ve received 5 paid and 2 additional committed student sponsorships. We signed up 4 new student members at UCCS on 28 April and have 1 additional student that we’ll get signed up separately. 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. You will be able to pay the fee via check to the chapter either in person or mail to me; Melody Wilson will get it deposited and then the chapter will sort out the payment process with ISSA International. Initially we’re focusing on UCCS and their Peak Chaos club. As I identify sponsorships, I’ll coordinate with UCCS to identify appropriate students to become members. 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 officially kicked off our 2014 membership drive with 36 new members in the first quarter of the year! We need at least another 45 new members to hit our recruiting goal for the year. Assuming we keep everyone renewing, that will put us over 400 members. The next membership drive activity is recruitment teams—start forming your 4-5 person teams and commit to bringing in 1 new member per recruitment team member. If we meet our Chapter goals, teams that meet their team goals will get a 1 year extension on each team member’s ISSA International membership (looks like you still have to pay your chapter dues, though). It’s really simple to do. Just send me the names in your recruitment team and identify one team member as the “lead”. All team members must be ISSA-COS members in good standing. When you sign someone up, all they have to do is list the recruiting team member’s name in the “referred by” block. The team leader notifies me and I track team status on the quarterly report. That’s all there is to it. Of course, referrals are also automatically entered in the ISSA International quarterly prize drawings that I mentioned in the February Newsletter.

As a separate activity, we’re trying to get a mentorship program off the ground. Several of our new student members have expressed an interest in having a mentor so we are looking for members interested in mentoring some of our new members. Please contact me if you’re interested.

Thanks for all your efforts and support.

David Reed
Membership Committee Chairman
dreed54321@att.net

(Continued from page 1)

industrialised, Oerting suggested. There is a growing market in exploits and hacks for sale, with groups developing cybercrime technology for use by their own associated criminal groups, or for sale on the open market. "Groups are developing malware so fast, that no protection can keep up," he noted.

When it comes to combatting cybercrime, law enforcement agencies face continued problems with jurisdiction and enforcement. It is not always clear whether the authorities in a jurisdiction can take action against a cyber criminal, and criminal groups are becoming ever more adept at hiding their location and identity, and concealing any electronic trail.

"If no crime originated in your country, how do you make sure you can bring an attacker to justice," asked Oerting. "If we wanted evidence, we would seize things. But in the very, very near future criminals will operate from the cloud, and they will stream their data. How do we then obtain evidence?"

Read the rest here:
Target Hackers May Take Years to Find

By Bree Fowler, Associated Press, April 17, 2014

Secret Service investigators say they are close to gaining a full understanding of the methods hackers used to breach Target's computer systems last December.

But the agency says it could take years to identify the criminals who stole some 40,000 debit and credit card numbers of Target shoppers and other personal information from as many as 70 million people in the pre-Christmas breach.

And it may take even longer to bring the offenders to justice. The federal investigation is complicated by the international nature of high-profile digital heists. The perpetrators are likely located overseas, which makes extradition and prosecution difficult. As a result, the Secret Service is focused on monitoring the online activities of its suspects, in hopes that they’ll be able to arrest them at an opportune moment, says Ari Baranoff, an assistant special agent in charge with the Secret Service's criminal investigative division.

"We take a lot of pride in having a lot of patience," Baranoff said during a rare sit-down interview with the Associated Press at the agency's headquarters in Washington. "There are individuals we've apprehended that we've known about for 10 years and we're very comfortable indicting these individuals, sitting back and waiting patiently until the opportunity arrives that we can apprehend them."

Target says it can’t yet estimate what the breach will cost the company, but some analysts put it at close to half a billion dollars. The total cost of the breach — which also would include losses incurred by banks, consumers and others — could easily reach into the billions of dollars.

Target, which is in the midst of its own investigation, has said very little about how the breach happened, except that it believes the thieves gained entry to its systems by infiltrating computers owned by one of its vendors, thought to be a Pittsburgh area heating and refrigeration business.

Baranoff couldn’t speak specifically about the federal investigation into the Target breach, since the case is ongoing, but he talked candidly about the growing threat of large-scale, financially motivated cyber crimes and the Secret Service’s efforts to stop them.

Behind every major breach, there’s usually a team of highly specialized cyber criminals who mainly know each other through online nicknames and reputations. Most aren’t motivated by politics, just greed, Baranoff says.

If the hackers do invest in anything, it’s their own operations. An increasing number are building their own server farms, sometimes leasing space to other criminals, making it harder for law enforcement to track them down.

Further complicating matters, Baranoff says the vast majority of high-level cybercriminals tend to be Russian speakers based in former Soviet and Eastern European countries, which largely puts them out of the reach of U.S. authorities.

But the Secret Service has strong ties with cybercrime agencies in many countries — including The Netherlands, Germany and the United Kingdom — and has found others to be helpful as well, even if they don’t have extradition treaties with the United States.

While best known for protecting the president of the United States, the U.S. Secret Service was originally formed in 1865 to investigate crimes related to counterfeit currency. The passage of the Patriot Act following the Sept. 11 terrorist attacks expanded its role in investigating computer-related crimes.

From the agency’s unassuming headquarters a few blocks from the bustle of the National Mall, special agents infiltrate online forums frequented by hackers, monitoring their activities, and creating online undercover identities in hopes of infiltrating criminal networks.

The same kinds of activities take place at the Secret Service’s other electronic crimes task forces in the U.S. and overseas. The tactics the investigators use are surprisingly similar to the law enforcement methods used by traditional beat cops everywhere. But digital investigations come with their own challenges. And based on the growing volume of stolen data now up for sale, hackers are becoming more sophisticated and more successful at evading justice.

Chester Wisniewski, senior security adviser for the computer security firm Sophos, says it’s the Secret Service’s ability to coordinate with law enforcement agencies around the world that make it effective in fighting cyber crime and help speed things up.

"With electronic crime, criminals move extremely fast and they’re dependent on the police being tied up in red tape," Wisniewski says.

Read the rest here:
The Colorado Springs Chapter of ISSA is hosting a 40-Hour CISSP Examination Preparation Seminar.

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

**Date:** May 17 2014

**Times:** Check in between 8:00 AM and 8:15 AM on Mar 22
*Class starts on the dates provided and runs from 8:15 AM to 4:45 PM each day (30 min lunch)*

**Cost:**
- Non ISSA and Trial Members - $500
- Current ISSA Members (not ISSA-COS) - $210
- Current CTU CSS 200 students - $175
- Current ISSA-COS members - $125
- Current ISSA-COS members who are also Current CSS 200 Students $100

ISSA members, who have already taken the class but would like to attend as a refresher, please contact Colleen Murphy for tuition rates.

**Registration & Volunteer Instructors Contact:**

Volunteers for instructors and support staff may contact Colleen Murphy at: crmurphy.cs@hotmail.com or Russ Weeks at: scoutguy@gmail.com.

To register for class provide your name, contact info, ISSA member number and student status to Colleen Murphy or Russ Weeks. Questions; please call Colleen at: 719-651-0415.

**Updated Course Content and In-Chapter Instructors**

- Updated and expanded material - CISSP Test Objectives & Exam Tips
- Each block of instruction covers the exam objectives

*All Instructors are CISSP Certified*

**Topics covered include**

- Access Control
- Information Security Governance and Risk Mgt
- Cryptography
- Operations Security
- Legal, Regulations, Investigations and Compliance
- Telecommunications and Network Security
- Software Development Security
- Security Architecture and Design
- Business Continuity and Disaster Recovery Planning
- Physical (Environmental) Security

**TO BECOME A MEMBER OF ISSA visit:** www.issa.org/ Join ISSA.
Specify the Colorado Springs Chapter.
How Heartbleed transformed HTTPS security into the stuff of absurdist theater

By Dan Goodin, ArsTechnica, April 21, 2014

If you want to protect yourself against the 500,000 or so HTTPS certificates that may have been compromised by the catastrophic Heartbleed bug, don't count on the revocation mechanism built-in to your browser. It doesn't do what its creators designed it to do, and switching it on makes you no more secure than leaving it off, one of the Internet's most respected cryptography engineers said over the weekend.

For years, people have characterized the ineffectiveness of the online certificate status protocol (OCSP) as Exhibit A in the case that the Internet's secure sockets layer and transport layer security (TLS) protocols are hopelessly broken. Until now, no one paid much attention. The disclosure two weeks ago of the so-called Heartbleed bug in the widely-used OpenSSL cryptography library has since transformed the critical shortcoming into a major problem, the stuff of absurdist theater. Security experts admonish administrators of all previously vulnerable websites to revoke and reissue TLS certificates, even as they warn that revocation checks in browsers do little to make end users safer and could indeed weaken the security and reliability of the Internet if they were made more effective.

Certificate revocation is the process of a browser or other application performing an online lookup to confirm that a TLS certificate hasn't been revoked. The futility of certificate revocation was most recently discussed in a blog post published Saturday by Adam Langley, an engineer who was writing on his own behalf but who also handles important cryptography and security issues at Google. In the post, Langley recites a litany of technical considerations that have long prevented real-time online certificate revocations from thwarting attackers armed with compromised certificates, even when the digital credentials have been recalled. Some of the considerations include:

- Attacks that use compromised or fraudulently issued TLS certificates more often than not are premised on the hacker's ability to intercept traffic passing between the target and the open Internet. This capability means attackers can use a mechanism known as OCSP stapling to retransmit a previous response signed by the OCSP server showing a certificate is valid, even though the real OCSP server, if the victim could reach it, would report it as revoked.
- Even in cases of domain name system hijacking and other hacks that allow attackers to intercept only traffic from a specific site, attackers can often cache thwart OCSP by saving a valid response issued earlier for the targeted website and presenting it along with a compromised certificate. What's more, if attackers have hijacked a website, there's a good chance they can use that control to trick a recognized certificate authority into issuing a TLS certificate for it.
- Most crucially, virtually all websites and browser makers prefer certificate revocations to work with what security engineers call a soft error, or "soft fail", rather than a "hard fail." A soft fail permits an HTTPS connection to be established even if the OCSP server isn't currently available to confirm a certificate's validity, whereas a hard fail would reject the connection. The reason for the soft fail default is that the Internet isn't reliable enough to guarantee OCSP servers are always available. If end users visiting PayPal, Amazon, or countless other websites get hung up waiting for OCSP checks, frustration on an unprecedented scale would almost certainly ensue. What's more, switching to a hard fail mechanism would give miscreants waging denial of service attacks a potent new weapon for taking down huge swaths of the Internet. Rather than overwhelm the sites themselves, the attackers would only need to target the much smaller pool of OCSP servers that validate the sites' certificates.

"That's why I claim that revocation checking is useless—because it doesn't stop attacks," Langley wrote. "Turning it on does nothing but slow things down. You can tell when something is security theater because you need some absurdly specific situation in order for it to be useful."

Read the rest here:
Edmonds Community College offers data recovery for Oso mudslide Victims

By Edmonds Community College, April 24, 2014

Edmonds Community College (Lynnwood, Washington) digital forensics and advanced data recovery students and faculty are volunteering to help recover data for the Oso mudslide victims.

"The students will perform the data recovery in the college's state-of-the-art digital forensics lab and cleanroom," said Steve Hailey, Edmonds CC Information Security and Digital Forensics instructor. "Even if a computer has been submerged in water and mud, we have the equipment and expertise to recover data from it."

As survivors, volunteers, and recovery teams search through the rubble left by the tragedy, they continue to locate and retrieve computers and other electronics. The possibility of recovering digital memories may offer a ray of hope.

"It's devastating enough to lose your home," said Hailey. "Ensuring the mudslide victims can recover their digital memories, irreplaceable family photos, and personal data is critical when so much has been lost. We're going to do everything we can to help."

As part of Edmonds CC's nationally recognized information security and digital forensics program, students learn to recover data from hard drives that have been severely damaged.

According to Hailey, recovering data from damaged hard drives can cost thousands of dollars per drive, depending on the severity of the damage and the methods that need to be used to recover the data.

Edmonds CC students Rob Matthews and Quincy Powell will be the college's liaisons with the Oso mudslide victims, responsible for the intake of the hard drives and overall coordination of the data recovery efforts.

"The digital forensic and data recovery skills we have developed at Edmonds CC are being put to great use," said Matthews. "We feel privileged to be able to restore digital photos, documents, and other data that might otherwise be lost for those affected by the mudslide."

Led by Hailey and instructor Mike Andrew, the hard drives will be triaged by students and members of the High Technology Crime Investigation Association — a non-profit organization devoted to the prevention, investigation, and prosecution of crimes involving advanced technologies — performing the initial diagnostics. The most severe cases will be escalated to the advanced data recovery students, led by instructor Richard Leickly.

About Our Instructors

Hailey and Andrew are internationally recognized subject-matter experts in digital forensics and information security and have taught classes for the Department of Homeland Security and the Federal Emergency Management Agency. Both have trained Department of Defense personnel tasked with analysis of digital evidence and intelligence in the Middle East. Both are also adjunct instructors for Texas A&M University and serve as officers of the Washington State High Technology Crime Investigation Association.

Leickly, co-owner and founder of the data recovery company Circle Hook, has recovered data for law enforcement agencies as well as the Department of Justice. He developed the curriculum currently being taught at the college for advanced data recovery students and has instructed members of local and federal law enforcement agencies in advanced data recovery techniques.
CryptoDefense ransomware leaves decryption key accessible

By Jeremy Kirk, ComputerWorld, April 1, 2014

A malicious software program that encrypts a person's files until a ransom is paid has a crucial error: it leaves the decryption key on the victim's computer.

Symantec analyzed a program called CryptoDefense, which appeared late last month. It's one of an extensive family of malware programs that scramble a person's files until a pricey ransom is paid, a long-running but still profitable scam.

CryptoDefense uses Microsoft's infrastructure and Windows API to generate the encryption and decryption keys, Symantec wrote on its blog.

Files are encrypted by CryptoDefense using a 2048-bit RSA key. The private key needed to decrypt the content is sent back to the attacker's server until the ransom is paid.

But CryptoDefense's developers apparently did not realize that the private key is also stashed on the user's computer in a file folder with application data.

"Due to the attacker's poor implementation of the cryptographic functionality they have quite literally left their hostages with a key to escape," Symantec wrote.

The decryption key may have been left under the door mat, but it's doubtful an average user infected with CryptoDefense would have the technical skills to figure it out.

CryptoDefense has been seen sent out in spam messages, masquerading as a PDF document. If a user installs it, the malware tries to communicate with four domains and uploads a profile of the infected machine, Symantec wrote.

It then encrypts files, inserting an additional file in folders with encrypted ones with instructions for how to free the files. The attackers have created a "hidden" website to receive payments using the TOR (The Onion Router) network, an anonymity tool.

TOR offers users a greater degree of privacy when browsing the Internet by routing encrypted traffic between a user and a website through a network of worldwide servers. TOR can also be used to host websites on a hidden network that can only be viewed through a web browser configured to use it.

The extortionists demand either US$500 or at least $500 within four days. If the victim doesn't pay in that time frame, the ransom doubles.

Since the ransom is payable in bitcoin, Symantec looked at the virtual currency's public ledger, called the blockchain, to see how many bitcoins have flowed into their coffers.

Read the rest here:
http://www.computerworld.com/s/article/9247348/CryptoDefense_ransomware_leaves_decryption_key_accessible

Explosion in Advanced Evasion Techniques and APTs Is Costing Businesses Millions

By Information Security Magazine, April 1, 2014

Misunderstandings, misinterpretation and ineffective safeguards in use by the security experts charged with protecting sensitive data have led to both controversy and confusion surrounding advanced evasion techniques (AETs), and the role that they play in advanced persistent threats (APTs).

With the average cost of a data breach to an organization coming in at upwards of $1 million, it's imperative to take a realistic tack when it comes to understanding and thwarting AETs, according to a Vanson Bourne study, commissioned by McAfee.

AETs, first discovered in 2010 by network security specialist Stonesoft (acquired by McAfee last year), are methods of disguise used to penetrate target networks undetected and deliver malicious payloads. Using AETs, an attacker can split apart an exploit into pieces, bypass a firewall or IPS appliance, and once inside the network, reassemble the code to unleash malware and continue an APT attack. The prevalence of these techniques has risen significantly since 2010, with millions of combinations and modifications of network-based AETs having been identified to date.

The report found that more than one in five security professionals admit their network has been breached (22%), and out of those, nearly 40% believe that AETs played a key role. However, the scope of the AET threat is often widely underestimated – the report shows that respondents believe there are less than 500,000 of them. In reality, there are an estimated 800 million known AETs. And less than 1% are detected by other vendor's firewalls.

Read the rest here:
The ISSA Colorado Springs Chapter is looking for volunteers for the following positions:

1. Security+ Review Seminar Coordinator

Duties:

Recruit and schedule instructors. Coordinate review of course content and accompanying PowerPoint slides. Coordinate printing of PowerPoint slides and provide to students at each session. Proctor review sessions. Coordinate with ISSA Training Team registrar and refreshments coordinator to communicate class size for planning/preparation purposes. Help set up class room for instructors. Respond to registering student queries as needed.

We currently hold three Security+ review seminars each calendar year; the first Saturday of March, June, and September. If the first Saturday happens to be a holiday, we divert to the second Saturday. Your duties will include coordinating the June 7, 2014, Security+ session.

2. Security+ Instructor

Duties:

We need instructors for the **7 Jun 2014** Security+ Review Seminar for the following topics:

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

We provide you our baseline slides for instruction, but you may modify as you see fit as long as your changes remain within official CompTIA content. During the review seminar, each topic consist of no more than 1.25 hours of instruction. Scheduling of time slots is completed through the Security+ Review Seminar Coordinator. We have a policy that instructors be Security+ Certified, but can work with individuals on a case by case basis if needed.

If you are interested in either the coordinator or an instructor position, please contact:

Jim Stephens (*jstephens22@comcast.net*) or Colleen Murphy (*crmurphy.cs@hotmail.com*).
ISSA-COS Training Team at Work
Crimeware Helps File Fraudulent Tax Returns

By Brian Krebs, KrebsonSecurity, April 14, 2014

Many companies believe that if they protect their intellectual property and customers’ information, they’ve done a decent job of safeguarding their crown jewels from attackers. But in an increasingly common scheme, cybercriminals are targeting the Human Resources departments at compromised organizations and rapidly filing fraudulent federal tax returns on all employees.

Last month, KrebsOnSecurity encountered a Web-based control panel that an organized criminal gang has been using to track bogus tax returns filed on behalf of employees at hacked companies whose HR departments had been relieved of W2 forms for all employees.

According to the control panel seen by this reporter, the scammers in charge of this scheme have hacked more than a half-dozen U.S. companies, filing fake tax returns on nearly every employee. At last count, this particular scam appears to stretch back to the beginning of this year’s tax filing season, and includes fraudulent returns filed on behalf of thousands of people — totaling more than $1 million in bogus returns.

The control panel includes a menu listing every employee’s W2 form, including all data needed to successfully file a return, such as the employee’s Social Security number, address, wages and employer identification number. Each fake return was apparently filed using the e-filing service provided by H&R Block, a major tax preparation and filing company. H&R Block did not return calls seeking comment for this story.

Fraudulent returns listed in the miscreants’ control panel that were successfully filed produced a specific five-digit tax filing Personal Identification Number (PIN) apparently generated by H&R Block’s online filing system. An examination of the panel suggests that successfully-filed returns are routed to prepaid American Express cards that are requested to be sent to addresses in the United States corresponding to specific “drops,” or co-conspirators in the scheme who have agreed to receive the prepaid cards and “cash out” the balance — minus their fee for processing the bogus returns.

Alex Holden, chief information security officer at Hold Security, said although tax fraud is nothing new, automating the exploitation of human resource systems for mass tax fraud is an innovation.

“The depth of this specific operation permits them to act as a malicious middle-man and tax preparation company to be an unwitting ‘underwriter’ of this crime,” Holden said. “And the victims maybe exploited not only for 2013 tax year but also down the road, and perhaps subject of higher scrutiny by IRS — not to mention potential financial losses. Companies should look at their human resource infrastructure to ensure that payroll, taxes, financial, medical, and other benefits are afforded the same level of protection as their other mission-critical assets.”

I spoke at length with Doug, a 45-year-old tax fraud victim at a company that was listed in the attacker’s control panel. Doug agreed to talk about his experience if I omitted his last name and his employer’s name from this story. Doug confirmed that the information in the attacker’s tax fraud panel was his and mostly correct, but he said he didn’t recognize the Gmail address used to fraudulently submit his taxes at H&R Block.

Doug said his employer recently sent out a company-wide email stating there had been a security breach at a cloud provider that was subcontracted to handle the company’s employee benefits and payroll systems.

“Our company sent out a blanket email saying there had been a security breach that included employee names, addresses, Social Security numbers, and other information, and that they were going to pay for a free year’s worth of credit monitoring,” Doug said.

Almost a week after that notification, the company sent out a second notice stating that the breach extended to the personal information of all spouses and children of its employees.

“We were later notified that the breach was much deeper than originally suspected, which included all of our beneficiaries, their personal information, my life insurance policy, 401-K stuff, and our taxes,” Doug said. “My sister-in-law is an accountant, so I raced to her and asked her to help us file our taxes immediately. She pushed them through quickly but the IRS came back and said someone had already filed our taxes a few days before us.”

Read the rest here: http://krebsonsecurity.com/2014/04/crimeware-helps-file-fraudulent-tax-returns/
Five-year-old discovers Xbox password bug, hacks dad's Live account

By Iain Thomson, The Register, April 4, 2014

Transferring data onto your computer could soon be as simple as using a post-it note.

The parents of Kristoffer Von Hassel, from Ocean Beach in San Diego, California, noticed after Christmas that the talented tot had broken into the account without knowing the password — allowing him to cheekily play games for adults that he wasn’t supposed to touch.

The kid managed it by tapping in a wrong password at the console’s login prompt, navigating to a password verification screen, and filling the password box with space characters before hitting the submit button. After that, the door was open.

“I was like, ‘yea!’” Kristoffer told ABC News.

His father Robert Davies, who works as a computer security specialist, said the inquisitive infant has a record of doing this kind of thing. When Kristoffer was one year old, he defeated the toddler lock on his dad’s phone by holding the home key down to disable the lockout — but the Xbox hack is the kid’s best discovery to date, his father said.

“How awesome is that!” Davies said. “Just being five years old and being able to find a vulnerability and latch onto that. I thought that was pretty cool.”

Davies got in touch with Redmond and the problem has been fixed, allowing the family to go public with the discovery. Kristoffer received four games for free from Microsoft in recompense, along with a year’s Xbox Live subscription and $50 (about 30 quid), as well as a mention on the company’s vulnerabilities shoutout web page.

Read the rest here:
http://www.theregister.co.uk/2014/04/04/five_year_olds_xbox_live_passwordHack/
Everybody – at least every multinational that Cisco checked out for its 2014 Annual Security Report – is hosting malware of some kind, and there aren't enough security professionals to go around.

Along with its Managed Threat Defense service launched this week, Cisco also launched the latest publication of its security survey. The study claims that “100 percent of companies [in the report's sample – *El Reg*] are calling malicious malware hosts”.

Cisco also believes that the length of time that such activity persists means that network penetrations are going undetected.

The research comes from a decent whack of statistics, according to the company's description of its sampling, which each day covers 16 billion Web requests, 93 billion e-mails, 200,000 IP addresses, 400,000 malware samples, 33 million files from endpoints and 28 million network connections.

Java is the undisputed king of endpoint vulnerabilities, Cisco claims, with far more exploits than either Flash or PDF: 91 per cent of the live endpoint exploits detected by the Sourcefire FireAMP system attacked Java. Adobe Reader only managed 3 per cent of detections (equal to Excel), with Word exploits at 2 per cent and PowerPoint exploits at 1 per cent.

Read the rest here:
http://www.theregister.co.uk/2014/04/24/cisco_youre_all_malware_hosts/

---

**Common interview mistakes that cost you the job**

By Dan Morrison, Careerealsim, April 14, 2014

Be better prepared for your next interview by avoiding the following common mistakes.

1) **You Neglect Your Cover Letter:** There's nothing more important than your cover letter—not even your resume.

2) **You Try Too Hard:** You should display confidence, but it's important to remember that there's a fine line between confidence and ego.

3) **You Keep Going, And Going:** Do not talk over the interviewer. If you catch yourself doing this, don't persist. Stop, let the other person finish speaking, and then try again.

4) **You Badmouth Your Previous Employer:** No matter how you feel about your last job, check that negativity at the door and come in armed with a more appropriate answer to the question, "Why did you leave your last job?"

5) **You Flunk The Salary Negotiation:** Mentioning money early on in an interview can cause doors to close. You need to sell yourself before you can set a price.

6) **You Lack Enthusiasm About the Job:** The candidate who gets the job is the one that does their research, demonstrating a strong desire to do good work for a potential employer.

7) **You Don't Explain Triumphs:** Show, don't tell. Tell the interviewer a story about how you used a skill to accomplish something for a prior employer.

8) **You're Desperate--And It Shows:** Over-eagerness can backfire in an interview, and it's often paired with anxious rambling that bores and annoys interviewers.
Quantum cryptography for mobile phones

An ultra-high security scheme that could one day get quantum cryptography using Quantum Key Distribution into mobile devices has been developed and demonstrated by researchers from the University of Bristol’s Centre for Quantum Photonics (CQP) in collaboration with Nokia.

By University of Bristol (UK), April 3, 2014

The Green Party recently called on the government to sign up to an accord that ensures financial transactions between the government and oil, gas and mineral companies are made public.

Secure mobile communications underpin our society and through mobile phones, tablets and laptops we have become online consumers. The security of mobile transactions is obscure to most people but is absolutely essential if we are to stay protected from malicious online attacks, fraud and theft.

Currently available quantum cryptography technology is bulky, expensive and limited to fixed physical locations – often server rooms in a bank. The team at Bristol has shown how it is possible to reduce these bulky and expensive resources so that a client requires only the integration of an optical chip into a mobile handset.

The scheme relies on the breakthrough protocol developed by CQP research fellow Dr Anthony Laing, and colleagues, which allows the robust exchange of quantum information through an unstable environment. The research is published in the latest issue of Physical Review Letters.

Dr Laing said: “With much attention currently focused on privacy and information security, people are looking to quantum cryptography as a solution since its security is guaranteed by the laws of physics. Our work here shows that quantum cryptography need not be limited to large corporations, but could be made available to members of the general public. The next step is to take our scheme out of the lab and deploy it in a real communications network.”

The system uses photons – single particles of light – as the information carrier and the scheme relies on the integrated quantum circuits developed at the University of Bristol. These tiny microchips are crucial for the widespread adoption of secure quantum communications technologies and herald a new dawn for secure mobile banking, online commerce, and information exchange and could shortly lead to the production of the first ‘NSA proof’ mobile phone.

Read the rest here:

(ISC)^2 Offers Cyber Forensics Certification in Europe

By (ISC)^2, April 16, 2014

(ISC)^2 ("ISC-squared") has announced the availability of its Certified Cyber Forensics Professional – European Union (CCFPSM-EU) certification in Europe.

The CCFP is the only global standard currently available for assessing experienced digital forensics professionals’ mastery of the discipline. Originally only available for the U.S. and South Korea, the credential has been developed for the European legal environment following a series of exam workshops conducted by a panel of experts from public and private sector organizations in the UK and Europe to ensure that its scope and content reflects the requirements of the region.

The CCFP is an expert-level credential that offers a common, internationally recognized body of knowledge. It exposes a comprehensive, yet advanced knowledge that today’s experienced cyber forensics practitioners must demonstrate. Many of the existing certifications available today are of a foundational level and focus on a narrow aspect of the cyber forensics realm.

“A major challenge for the information security community today is that we are unable to fight cybercrime as one force,” explains Lorenz Kuhlee, CCFP-EU, (ISC)^2 volunteer and lead investigator for the RISK Team at Verizon.

“The crime scene is broad and so to be effective, there is a need for collaboration across the cybercrime landscape in a way that bridges all aspects of security including technology, analytics, law enforcement and business. In Europe, the complexity is much higher due to the law-related disparities among countries. The CCFP credential supports the unique requirements of individual countries, but equips professionals with a best practice-led, uniform and thorough approach to dealing with overall challenges,” he said.

The CCFP spans the digital forensics and information security disciplines. The six (ISC)^2 CBK domains within the credential include:

- Legal & Ethical Principles
- Investigations
- Forensic Science
- Digital Forensics
- Application Forensics
- Hybrid & Emerging Technologies

Read the rest here:
Is the US headed toward a cyber Cold War with China?

Harvard scholar suggests the superpowers are locked in a "cool war."

By Joe Silver, ArsTechnica, April 9, 2014

Are cyberattacks, security breaches, and mounting distrust between the US and Chinese governments ushering in a new Cold War era? Given US officials’ rhetoric and actions in recent months, it might appear that such a sustained state of political and military tensions between the two superpowers is a serious threat.

A number of events have likely precipitated Cold War fears. The disclosures by National Security Agency whistleblower Edward Snowden of dragnet government surveillance, including a revelation that the US has infiltrated the networks of China-based telecommunications company Huawei, have understandably upset the Chinese. Additionally, the increasing number of cyberattacks and security breaches in both the US and China appear to have strained relations.

And considering the “mounting tensions over China’s expanding claims of control over what it argues are exclusive territories in the East and South China Seas, and over a new air defense zone,” diplomatic relations between the two countries appear further strained, according to a report from The New York Times.

“A cool war”

But while US officials are trying to fend off threats of a new Cold War, Harvard Law School scholar Noah Feldman described his belief that rather than entering a new Cold War period, the US and China are instead enmeshed in what he calls a “cool war.”

“What the US and China have in common is that each is a global superpower in a contest for geopolitical supremacy,” Feldman told Ars. “What makes it ‘cool’ and not cold is that we still have a strong economic partnership with China. While both sides would like to reduce their dependence on the other, neither side wants escalation.”

Feldman said that the two countries have been toeing a delicate diplomatic line since revelations of spying and cyberwarfare have emerged. The Snowden leaks, such as the NSA’s hacking into Chinese network giant Huawei, have created greater tension that neither country wants. The Chinese government, he said, fears a strong nationalist backlash to such revelations.

Easing tensions

What’s more, in an apparent effort to smooth over relations between the US and Chinese governments, the Obama administration has held a series of unprecedented briefings for the Chinese military leadership, as described in the New York Times report. Specifically, US officials have met with Chinese leaders to share information regarding America’s policies both for defending against cyberattacks and in using cyber technologies against adversaries, as outlined by the Associated Press.

American officials have analogized their actions to Cold War-era exchanges held with the Soviets so that each side understands the “red lines” for employing nuclear weapons against each other. “Think of this in terms of the Cuban missile crisis” a senior Pentagon official told the Times. “The last thing we would want to do is misinterpret an attack and escalate to a real conflict.”

Feldman suggested that the US government’s willingness to provide some information to China regarding its cyber strategies and China’s apparent refusal to reciprocate by offering its own information are strategic diplomatic responses. He believes the two superpowers have devised this tactic in order to give the appearance that actions are being taken to address US intelligence overreach, when in fact “this is a purely symbolic gesture” intended to quell a nationalist uprising in China. Feldman elaborated:

We all are going to have to get used to the rules of the new game. The rules are being made up as we go along. What two countries do when a third party reveals their spying efforts. The two sides are engaged in a delicate dance... trying to figure out how to continue doing cyberattacks. Neither wants escalation because both sides have too much to lose by unsettling the status quo.

Read the rest here:

Why There Will Be A Robot Uprising

By Patrick Tucker, DefenseOne, April 17, 2014

In the movie Transcendence, which opens in theaters on Friday, a sentient computer program embarks on a relentless quest for power, nearly destroying humanity in the process.

The film is science fiction but a computer scientist and entrepreneur Steven Omohundro says that “anti-social” artificial intelligence in the future is not only possible, but probable, unless we start designing AI systems very differently today.

Omohundro’s most recent recent paper, published in the Journal of Experimental & Theoretical Artificial Intelligence, lays out the case.

We think of artificial intelligence programs as somewhat humanlike. In fact, computer systems perceive the world through a narrow lens, the job they were designed to perform.

Microsoft Excel understands the world in terms of numbers entered into cells and rows; autonomous drone pilot systems perceive reality as a bunch calculations and actions that must be performed for the machine to stay in the air and to keep on target. Computer programs think of every decision in terms of how the outcome will help them do more of whatever they are supposed to do. It’s a cost vs. benefit calculation that happens all the time. Economists call it a utility function, but Omohundro says it’s not that different from the sort of math problem going in the human brain whenever we think about how to get more of what we want at the least amount of cost and risk.

For the most part, we want machines to operate exactly this way. The problem, by Omohundro’s logic, is that we can’t appreciate the obsessive devotion of a computer program to the thing it’s programed to do.

Put simply, robots are utility function junkies.

Read the rest here:

Upcoming Chapter Meetings

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 14</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>May 22</td>
<td>5:45 to 8:00</td>
<td>TREA</td>
</tr>
<tr>
<td>June 11</td>
<td>10:45 to 1:00</td>
<td>TREA</td>
</tr>
<tr>
<td>June 19</td>
<td>5:45 to 8:00</td>
<td>TREA</td>
</tr>
<tr>
<td>July 9</td>
<td>10:45 to 1:00</td>
<td>TREA</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>
News Ripped From the Headlines

April 2, Softpedia – (International) Cybercriminals abuse security camera recorders and routers to mine for Bitcoins. A researcher at the SANS Technology Institute identified malware designed to infect security camera recorders and routers and use the devices to attempt to mine Bitcoin virtual currency. The malware is designed to run on ARM infrastructure and was spotted on Hikvision DVRs, which have a simple default root password that users often do not change. Source: http://news.softpedia.com/news/Cybercriminals-Abuse-Security-Camera-Recorders-and-Routers-to-Mine-for-Bitcoins-435427.shtml

April 3, Softpedia – (International) Cybercriminals add new component to Sality to hijack the DNS addresses of routers. Researchers at ESET analyzed a new component of the Sality malware that was recently added and allows the malware to hijack the primary DNS address of routers. The analysis showed that the malware targets specific router models and attempts to use a brute force attack to gain administrator access, and then changes the router’s DNS server address in order to direct users to fake installation sites. Source: http://news.softpedia.com/news/Cybercriminals-Add-New-Component-to-Sality-to-Hijack-the-DNS-Addresses-of-Routers-435654.shtml

April 3, Softpedia – (International) ISPs exposed to DNS DDoS attacks due to millions of vulnerable home routers. Researchers at Nominum reported finding over 5.3 million routers have open DNS proxies, which can put Internet service providers at risk of DNS amplification distributed denial of service (DDoS) attacks. Source: http://news.softpedia.com/news/ISPs-Exposed-to-DNS-DDOS-Attacks-Due-to-Millions-of-Vulnerable-Home-Routers-435608.shtml

April 10, Softpedia – (International) Deltek suffers data breach, hackers gain access to credit card information. Deltek reported that attackers breached the company’s GovWin IQ Web site, exposing personal and financial details of around 80,000 employees of federal contractors and about 25,000 payment card details belonging to customers of the site’s eCommerce platform. The breach was first discovered March 13 but occurred sometime between July 3, 2013 and November 2, 2013. Source: http://news.softpedia.com/news/Deltek-Suffers-Data-Breach-Hackers-Gain-Access-to-Credit-Card-Information-436861.shtml

April 14, Softpedia – (International) Flash SMS flaw in iOS can be exploited to make the lock screen unresponsive. A security researcher identified a Flash SMS flaw in iOS that can be used to make a device’s lock screen unresponsive, which could be used for ransom attacks. The flaw was fixed with the release of iOS 7.1 but devices running previous versions of the mobile operating system are vulnerable. Source: http://news.softpedia.com/news/Flash-SMS-Flaw-in-iOS-Can-Be-Exploited-to-Make-the-Lock-Screen-Unresponsive-437566.shtml

April 17, Help Net Security – (International) Attackers use reflection techniques for larger DDoS attacks. Akamai released a global distributed denial of service (DDoS) attack report, which found that attackers in the first quarter of 2014 favored using reflection and amplification techniques to conduct DDoS attacks, rather than relying on aditional botnets. The report found that the most abused protocols were Character Generator (CHARGEN), Network Time Protocol (NTP), and Domain Name System (DNS). Source: http://www.net-security.org/secworld.php?id=16707

A range of crucial satellite systems manufactured by some of the world’s biggest government contractors contain severe vulnerabilities that could be exploited to disrupt military operations and flight-safety communications, researchers have warned.

Security consultancy IOActive says it has uncovered various vulnerabilities in software and ground-based satellite systems manufactured by British suppliers Cobham and Inmarsat. US firms Harris Corporation, Hughes and Iridium were also said to have produced vulnerable kit, alongside Thuraya, a UAE provider, and Japan Radio Company.

The Computer Emergency Response Team based in Carnegie Mellon University, which is sponsored by the Department of Homeland Security, warned about a handful of the vulnerabilities in January. But on Wednesday information on more alleged weaknesses was released, amid growing concern the contractors are ignoring the threats. The latest report from IOActive suggested there were some easily hackable systems, many of which were designed for keeping aircraft, ships and army personnel safe.

Many of the issues lie in the Broadband Global Area Network (BGAN) satellite receivers that the manufacturers produce with Inmarsat, the satellite operator that provided tools vital in helping locate the Malaysian passenger plane MH370 that crashed last month. BGAN is designed to provide internet and voice connectivity for remote teams.

The affected Harris BGAN satellite terminals are used by the military, including Nato, for tactical radio communications. Thanks to the vulnerabilities, a hacker could install malicious software on the devices to obtain the location of the soldiers using the kit, or even disable the systems, according to IOActive.

Cobham produces most Inmarsat terminals, a handful of which were found to be vulnerable. Those used in shipping, such as the Ship Security Alert System, could be exploited to prevent vessels detecting distress messages or direct those containing sensitive cargo on a collision course, suggested Ruben Santamarta, the IOActive researcher who found the alleged weaknesses.

The Cobham Aviator machines could be compromised to alter satellite communications, such as the Aircraft Communications Addressing and Reporting System (Acars), used by a plane, he added.

Acars, which is used to transmit vital information such as fuel levels, was initially used to track the movements of the MH370 flight soon after it disappeared, before Inmarsat stepped in to help. Attacks on the Cobham aircraft systems could “pose a safety threat for the entire aircraft”, IOActive’s advisory read.

Only Iridium had confirmed it was working on fixes for the vulnerabilities. None of the other manufacturers had responded to contact from the Cert, which had been informed of the issues by IOActive, Santamarta said.

Read the rest here: http://www.theguardian.com/technology/2014/apr/17/military-satellite-system-vulnerable-hacking

By Tom Brewster, The Guardian (UK), April 17, 2014

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!
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.

The First Emoticon?
By Ria Misra, io9, April 14, 2014

Depending on who you’re talking to, emoticons have been adding drama to our typefaces since 1982, possibly even as early as the late 1960s. But was the emoticon actually invented 300 years earlier by an English poet?

Over at The Atlantic Tech, they highlight Robert Herrick’s 1648 poem "To Fortune", which Levi Stahl argues on his blog contains the very first instance of an emoticon ever. Immediately following the poet’s assertion that he’ll be "smiling yet" there it is: a tiny smiling face mashed-up out of a colon and a single parenthesis.

Read the rest here: http://io9.com/is-this-smiley-face-from-1648-the-very-first-emoticon-1563043652