The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
6 March 2014

Purpose
Educate recipients of cyber events to aid in the protection of electronically stored corporate proprietary, DoD and/or Personally Identifiable Information from theft, compromise, espionage, and / or insider threat

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, Sandia Labs

Distribution
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings Credit is given to the NMCIWG for the compilation of open source data

March 4, Ann Arbor News – (Michigan) **More than 50 computers stolen in overnight break-ins at 2 Ann Arbor high schools.** Police are investigating after thieves broke into Ann Arbor Technological High School and Huron High School in Michigan March 4 and stole or damaged more than 50 computers. Source: http://www.mlive.com/news/ann-arbor/index.ssf/2014/03/more_than_50_computers_stolen.html

March 5, Help Net Security – (International) **New Android devices sold with pre-installed malware.** The founder of Marble Security reported finding data-stealing malware disguised as Netflix apps pre-installed on several customers' new Android devices. Several Samsung, Asus, LG, and Motorola phones and tablets were found with the pre-installed malware. Source: http://www.net-security.org/malware_news.php?id=2724

March 5, The Register – (International) **New design flaw found in crypto's TLS: Pretend to be a victim online.** Researchers with the French National Institute for Research in Computer Science and Control developed a new man-in-the-middle (MitM) attack against the Transport Level Security (TLS) protocol that can under certain conditions allow an attacker to intercept a user's login credentials and disguise themselves as the user on servers that accept the same credential. Source: http://www.theregister.co.uk/2014/03/05/tls_authentication_broken_again/

March 5, The Register – (International) **GNU security library GnuTLS fails on cert checks: Patch now.** An issue in the GnuTLS security library was identified that could allow any certificate to be accepted as legitimate, affecting hundreds of applications that use the library. Red Hat and GnuTLS issued patches for users and advised them to apply the patch promptly. Source: http://www.theregister.co.uk/2014/03/05/gnu_security_library_gnutls_fails_on_cert_checks_patch_now/

Cybersecurity concerns becoming a boardroom issue
Heise Security, 6 Mar 2014: The increasing frequency, sophistication, and business impact of cyber-attacks have pushed cybersecurity planning and protection from an operational concern of IT departments to a key theme on the strategic agenda of boards and CEOs. Senior levels of the business still face an information gap that makes it difficult for them to align investments in risk protection to the true strategic value of an organization's digital assets; this, according to a report by global business consulting firm Bain & Company. Statistics show that:

- The median cost of cybercrimes jumped 56 percent to $5.9 million per organization in 2011 over 2010, the most recent data available
- Web-based attacks during the same period increased to 4,500 per day, a 36 percent rise
- Mobile malware quadrupled in 2013, with Android attacks increasing by an astounding 26 times
- DDoS attacks increased 27 percent in the same period

- Financial motives now drive nearly 95 percent of cyber-attacks, placing the target squarely on strategic assets that can be monetized after a breach.

Every organization that has suffered a recent security breach, the report notes, has also already had some form of cybersecurity in place. Beyond that, too many organizations fail to align IT security capabilities with larger goals and overall risk appetite. The report points to disconnects between an organization's risk-management efforts and the development of necessary cybersecurity capabilities as a hidden cause behind the material causes of individual incidents, because business groups and IT often fail to discuss emerging threats or the relative importance of different kinds of digital assets. Instead, according to the Bain report, compliance obligations, not strategy implications, are the greatest driver for cybersecurity considerations for three-in-four CIOs. The finding demonstrates the over-reliance placed on operational approaches to security. To read more click **HERE**

Sally Beauty felled by a recent payment system hack

ThreatWatch, 6 Mar 2014: A batch of 282,000 stolen credit and debit cards went on sale in a popular cybercrime store, and at least three banks went online to buy back the cards they had previously issued to customers. To figure out where the hackers had found access to the credentials – they used a test known as the "common point of purchase." Where were all the cards used during the same period of time? The banks determined all the cards -- there were 15 total -- had been used within the last ten days at Sally Beauty locations across the country. Sally Beauty spokeswoman Karen Fugate said the company recently detected an intrusion into its network, but that neither company computer experts nor an outside forensics firm could find evidence that customer card data had been stolen from the company's systems. "Fugate said Sally Beauty uses an intrusion detection product called Tripwire, and that a couple of weeks ago — around Feb. 24 — Tripwire detected activity," KrebsOnSecurity reports. "Unlike other products that try to detect intrusions based on odd or anomalous network traffic, Tripwire fires off alerts if it detects that certain key system files have been modified." After a deconstruction of the methods used, an examination of network traffic, all company logs and all potentially accessed servers, "we found no evidence that any data got out of our stores," Fugate said. "But our investigation continues." All of the banks reported fraud occurring on cards shortly after they were used at Sally Beauty, in the final week of February and early March. To read more click **HERE**

US lawmakers call for data protection standards to avoid breaches

Computerworld, 6 Mar 2014: The U.S. Congress should mandate that banks, retailers and payment card processors adopt new security standards to protect against widespread data breaches, some lawmakers said Wednesday. In the wake of several high-profile retail data breaches, some members of the U.S. House of Representatives Financial Services Committee called for new cybersecurity mandates, with Representative David Scott, a Georgia Democrat, asking if Congress should require the U.S. financial industry to adopt new card security measures used in other countries. The U.S. payments and financial system makes "things easy for fraudsters" by relying on magnetic-strip credit and debit cards instead of moving to EMV cards that contain integrated computer chips and require customers to enter PINs at the point of purchase, Scott said. Congress is "anxious" to take action to stop data breaches, Scott said. During Wednesday's hearing, several lawmakers noted the data breach at retailer Target affecting up to 110 million U.S. residents. "Is there any reason Congress shouldn't mandate that payment card security standards use the most effective technology in the marketplace?" asked Scott. "I think this is a problem of soaring magnitude, and we're going to be in trouble if we don't get a handle on this." Congress should mandate higher standards, but lawmakers shouldn't mandate specific technologies, said Edmund Mierzwinski, consumer program director at consumer group U.S. PIRG (Public Interest Research Group). "We are still using a 40- or 50-year-old magnetic stripe obsolete technology," Mierzwinski said. "We are now starting to move slowly" to new technologies. Banks and payment processors have said that moving to a chip-and-PIN card system will be expensive, requiring new card-reading machines at all retailers. Visa, MasterCard and others have announced plans to move to chip-based cards by late 2015. Some lawmakers and witnesses called for a national data breach notification law, to supersede the 45-plus state laws now on the books. A national breach notification law would make it simpler for companies to comply with the requirements and simpler for consumers to understand the notifications, some representatives of the financial industry said. But a national data breach law shouldn't preempt tough state laws, Mierzwinski said. And it shouldn't, as some backers of a national law have suggested, allow companies to avoid reporting a data breach if they don't believe thieves have gained access to personal information. "Force companies that lost your information to tell us about it," he said. Other witnesses called for security standards to come from private industry. The PCI Security Standards Council, an organization that develops payment security standards, already has payment processing standards in place, including a standard for using chipped payment cards, said Troy Leach, CTO at the council. The U.S. government should focus on prosecuting cybercriminals and on encouraging threat information-sharing between businesses and government, Leach said. The development of payment card standards is "something we are uniquely qualified to do," he said. "The recent breaches underscore the complex nature of payment card security. The multifaceted problem cannot be solved by a single technology, mandate or regulation." Other lawmakers pressed representatives of the U.S. Secret Service and the U.S. Department of Homeland Security to more aggressively prosecute cybercrime. To read more click **HERE**

CIOs Battle Worker Apathy towards Lost or Stolen Mobile Phones

Network World, 5 Mar 2014: Like spoiled teenagers, American workers are telling their CIO that lost or stolen phones are simply not their fault, not their problem. Corporate data theft is no big deal. It's just a phone, they say. Besides, aren't you responsible for mobile data security? It's enough to make a CIO's blood boil. In a survey of 750 U.S. workers in industries such as banking, retail, healthcare and energy, conducted by Absolute Software in November, there appears to be a general feeling of apathy toward mobile security. In a survey of 750 U.S. workers in industries such as banking, retail, healthcare and energy, conducted by Absolute Software in November, there appears to be a general feeling of apathy toward mobile security. Even if employees leak or lose corporate data, 25 percent of respondents say it's not their problem. Of those who actually lost a phone, 34 percent were not punished, 30 percent had to replace the device and 21 percent simply had a "talkin' to." Given such lackadaisical responses, it's no surprise that one-third of respondents who had lost their phones did not change their security habits afterwards. Part of the problem is that employees don't really know what's at stake nor do they bother to understand the security portion of the user policy. In the survey, 59 percent estimated the value of the corporate data on their phones to be less than $500 -- although that's hardly the case. "If we end up on the front of the Fresno Bee because an attorney left his phone at the bar... the damage to your reputation could literally be millions of dollars," CIO Darin Adcock at California-based law firm **** Dowling Aaron, told CIO.com. **** To be fair, CIOs must shoulder some of the blame for workers being uniformed about mobile security user polices, which can get a little dense. One out of four workers doesn't know company procedure for dealing with work device loss or theft, according to the survey. It's a communication problem that's not solely the worker's fault. Additionally, CIOs say lots of employees will keep looking for a lost phone for weeks and not report it (although the policy says they should) out of fear it'll get wiped and they'll lose personal data. That's also perhaps a problem with the policy in relation to human behavior. "If firms don't set clear policies that reflect the priority of corporate data security, they can't expect employees to make it a priority on their own," says Tim Williams, mobile enterprise data expert at Absolute Software. But clear user policies aren't the only way to get employees to pay attention to the dangers of mobile data loss. Paul Luehr, managing director at Stroz Friedberg, a global data risk management company with a cyber-crime lab, told CIO.com that he's seen the fallout from a lack of consequences for poor security at the individual level. To read more click **HERE**

New technique targets C code to spot malware attacks

Heise Security, 6 Mar 2014: Researchers from North Carolina State University have developed a new tool to detect and contain malware that attempts root exploits in Android devices. The tool improves on previous techniques by targeting code written in the C programming language – which is often used to create root exploit malware, whereas the bulk of Android applications are written in Java. Root exploits take over the system administration functions of an operating system, such as Android. A successful Android root exploit effectively gives hackers unfettered control of a user's smartphone. The new security tool is called Practical Root Exploit Containment (PREC). It refines an existing technique called anomaly detection, which compares the behavior of a downloaded smartphone application (or app), such as Angry Birds, with a database of how the application should be expected to behave. When deviations from normal behavior are detected, PREC analyzes them to determine if they are malware or harmless "false positives." If PREC determines that an app is attempting root exploit, it effectively contains the malicious code and prevents it from being executed. "Anomaly detection isn't new, and it has a problematic history of reporting a lot of false positives," says Dr. Will Enck, an assistant professor of computer science at NC State and co-author of a paper on the work. "What sets our approach apart is that we are focusing solely on C code, which is what most – if not all – Android root exploits are written in." "Taking this approach has significantly driven down the number of false positives," says Dr. Helen Gu, an associate professor of computer science at NC State and co-author of the paper. "This reduces disturbances for users and makes anomaly detection more practical." The researchers are hoping to work with app vendors, such as Google Play, to establish a database of normal app behavior. Most app vendors screen their products for malware, but malware programmers have developed techniques for avoiding detection – hiding the malware until users have downloaded the app and run it on their smartphones. To read more click **HERE**

CIA, NSA and others tell utilities how to up their cybersecurity

SmartGridNews, 6 Mar 2014: The Bipartisan Policy Center (BPC) today published a new report through its Electric Grid Cybersecurity Initiative with recommendations on how to better prepare for cyber attacks against the electric grid. The report is authored by the initiative's co-chairs General (Ret.) Michael Hayden, former director of the Central Intelligence Agency and National Security Agency; Curt Hébert, former chairman of the Federal Energy Regulatory Commission (FERC) and former executive vice president of Entergy Corporation; and Susan Tierney, former assistant secretary for policy at the Department of Energy. Cyber attacks on key energy infrastructure, including the electricity system, are increasing in terms of frequency and sophistication. Electric grid failures are costly and have the potential to profoundly disrupt delivery of essential services, including communications, food, water, health care and emergency response. In light of these developments, BPC convened the Electric Grid Cybersecurity Initiative – a hybrid project of BPC's Energy and Homeland Security Projects – to tackle these challenges.   Although industry has taken many actions to prevent such attacks, there is more that can be done to improve grid cybersecurity. BPC's initiative identified urgent priorities, including strengthening existing protections, enhancing coordination at all levels and accelerating the development of robust protocols for response and recovery in the event of a successful attack. The initiative developed recommendations in four policy areas: standards and best practices, information sharing, response to a cyber attack and paying for cybersecurity. The recommendations are targeted to Congress, federal government agencies, state public utility commissions (PUCs) and industry. "Timely information sharing is the primary way to identify, assess and respond to threats in real time," said General Hayden. "The intelligence community needs to identify best practices for sharing classified information in a way that is actionable for industry.""The electric power industry is proactively taking many steps to protect the grid from cyber attacks, but current policy treats transmission and distribution systems very differently. Given the interconnectedness of the grid, there is a need to complement existing efforts with an organization that broadly encompasses a full set of power sector participants to advance cybersecurity risk-management practices," said Curt Hébert. "This organization – modeled after the nuclear industry's Institute for Nuclear Power Operations – could provide detailed facility evaluations, train and accredit related professionals, and provide technical and management assistance to individual utilities.""Utilities are expected to spend roughly $7 billion on cybersecurity by 2020. That's not chump change," said Susan Tierney. To read more click **HERE**

Two People Arrested for Hacking into KT Corp, Stealing Details of 12M Users
SoftPedia, 6 Mar 2014: South Korean police have arrested a couple of individuals suspected of hacking into the systems of KT Corp, one of the country's largest telecom companies. According to CNN, a man named Kim is said to have hacked into KT Corp's systems, stealing the personal details of 12 million customers. The stolen data included bank details, addresses and employment information. The data was later sold to a man named Park, the owner of a telemarketing company. Park posed as a KT Corp representative and used the stolen information to sell mobile phones. Since February 2013, when the scheme started, the two made 11.5 billion won ($10.8 million / €7.85 million). There's a third suspect in this case, but he has been released. KT is investigating the incident. The company is trying to determine who else might have obtained the leaked information. In late February, South Korean authorities arrested three men suspected of hacking into 225 websites and stealing the personal details of 17 million people. They're said to have sold the data for 100 million won ($93,000 / €68,657). Another major data breach affected the customers of major South Korean credit card companies. A temporary employee of the Korea Credit Bureau managed to steal over 100 million payment card records, 20 million of which he sold to marketing companies. To read more click **HERE**

Hackers Access ComiXology Database, Users Advised to Change Passwords
SoftPedia, 6 Mar 2014: Cloud-based digital comics platform ComiXology has been hacked. Users and comic book retailers that host ComiXology's portals on their sites are being advised to take measures. Bleeding Cool has obtained copies of the email notifications sent out to both users and retailers. It turns out that hackers have accessed a database containing customer information, including password hashes. "In the course of a recent review and upgrade of our security infrastructure, we determined that an unauthorized individual accessed a database of ours that contained usernames, email addresses, and cryptographically protected passwords," the emails read. Fortunately, payment information is not stored on the company's servers so it couldn't have been compromised. It's uncertain how well the passwords are encrypted, but users and retailers are asked to change them as a precaution. ComiXology says it has strengthened its security procedures and systems to avoid future incidents. As far as retailers are concerned, they're also encouraged to change their SMTP passwords and send their SMTP credentials to ComiXology if they want to email their users through the company's service. Some users have complained that the email notifications sent out by ComiXology look like phishing scams. They address recipients with a generic "Dear Comics Reader" and they come from comixology@e.comixology.com, which some see as suspicious. At the time of writing, the company's website appears to be inaccessible. ComiXology says it's looking into the downtime. To read more click **HERE**

Hackers Leak 1,000 Documents from Russian Defense Export Company Rosoboronexport
SoftPedia, 6 Mar 2014: Hackers of a group called the Russian Cyber Command have leaked around 1,000 documents allegedly stolen from Rosoboronexport (roe.ru), the only state intermediary agency for Russia's defense-related imports and exports. The hacktivists posted the following message next to a link pointing to the leaked files: "Taken into consideration recent Russian Government delusional attempts to start WWIII, we – Free from Putin – people of Russian Federation - Free computer renegades and outlaws from IT Security – have decided to initiate a true domestic CyberWar on Russian Military Enterprises and eventually we shall deliver critical infrastructure companies on which Russian Putin's Empire stands on." According to a statement posted on CyberGuerrilla.org, the hackers stole the files after hacking into the systems of India's embassy in Moscow. After accessing the embassy's networks, they sent a maliciously crafted email to Rosoboronexport's CEO. This is how they've allegedly breached the organization's servers. "Same way we have infected SUKHOI, OBORONPROM, GAZFLOT, RUSAL and VELES CAPITAL and many others, but we shall deliver them right after this very first leak," the hackers said. The data leak appears to be legitimate, but it's difficult to say for certain if it is. The files, totaling close to 500 Mb, have been uploaded to BayFiles. A preview of the leak has been published on imgur.com. Currently, the Russian military is occupying the Ukrainian peninsula of Crimea. However, reportedly, there's movement in cyberspace as well. On March 2, the Georgetown Security Studies Review revealed that there were indications that Russia launched cyber operations against Ukraine, just as it did back in 2008 when it invaded Georgia.

Experts noted that Crimea is vulnerable to cyberattacks due to the positioning of its Internet exchange points. "While it cannot yet be confirmed that Russia is, in fact, conducting cyber operations in the Crimean Peninsula, the international community should carefully monitor the situation. As the crisis develops, there are a number of indicators that would demonstrate that Russia is pursuing a cyberstrategy similar to the one it used in Georgia," they explained. Valentyn Nalivaichenko, the head of Ukraine's SBU security service, has confirmed that the members of the Ukrainian parliament have been targeted in an "IP-telephonic attack" for two days in a row. According to Reuters, Nalivaichenko revealed that illegal equipment was installed at telecoms firm Ukrtelecom at the entrance to Crimea in an effort to block the communications of officials, regardless of their political affiliation. Security services in Ukraine are working on addressing the issue. To read more click **HERE**

Researchers Analyze Chinese Mobile Cybercriminal Underground Market
SoftPedia, 6 Mar 2014: Lion Gu, a senior threat researcher with Trend Micro, has published a research paper on the Chinese mobile cybercriminal underground market. The report analyzes SMS spam services and other similar products being put up for sale on the underground market in China. The underground offerings analyzed by Gu include premium service abusers, SMS forwarders, iMessage spamming services and software, SMS spamming services and devices, app rank-boosting services, and phone number scanning services. Premium service abusers are very common. They represent one of the favorite methods used by cybercriminals to make a quick profit. These threats are designed to subscribe victims to premium SMS services without their knowledge. Normally, when users subscribe to such services they receive an SMS to alert them. To make sure they don't raise any suspicion, SMS Trojans are designed to intercept and delete the confirmation messages. SMS forwarders are also dangerous because they're designed to intercept text messages received by users and forward them to the cybercriminals. This could be very problematic, particularly because many users receive authentication on verification codes on their mobile phones. These codes could allow the attackers to access online banking accounts and other services. SMS spamming services and even SMS spamming devices are being offered on the Chinese underground market. For instance, GSM modems are used to send and receive text messages with multiple SIM cards. A 16-slot GSM modem can be used to send out close to 1,000 SMSs per hour. And if 1,000 messages per hour are not enough, spammers can use Internet short message gateways. If they want to make spam texts appear as if they're coming from special numbers to trick victims into believing they're real, they can use SMS servers. A complete SMS server kit costs around $7,400 (€5,400). Cybercriminals who want to target Apple customers can rely on iMessage spamming services and software that enable them to send messages to iPhone, iPad, iPod and Mac users. Such solutions are usually cheap. It costs $16 (€11.6) to send out 1,000 text messages. However, in order to send out SMS spam, cybercriminals need phone numbers. To make sure they send texts only to real numbers, they use phone number scanning services. For 100,000 valid numbers spammers have to pay only $16 (€11.6). For $160 (€116) they can buy 3 million phone numbers. The complete report, titled The Mobile Cybercriminal Underground Market in China, is available on Trend Micro's website (**LINK**). To read more click **HERE**

Microsoft Fixes OneDrive Error, Starts Offering an Extra 3GB of Storage to Users
SoftPedia, 6 Mar 2014: A couple of weeks ago when Microsoft officially relaunched SkyDrive as OneDrive, the company also debuted a special offer that allowed users who configured automatic camera backup options to work with the service to receive an additional of 3GB of storage space. However, many users didn't receive the extra space due to what seemed to be a bug affecting OneDrive globally, but it turns out that Redmond has managed to determine the cause of the issue and repair it so that all users could receive the extra space. "Due to an error on our part, it took longer than expected for some of you to see the extra 3 GB in your OneDrive account. For that, we sincerely apologize. We pride ourselves on providing you, our best customers, with a seamless and dependable service," Microsoft said in a statement submitted to Microsoft News. "We're sorry for any stress and frustration that our mistake may have caused, and we've worked hard to make sure that if you're backing up your camera roll to OneDrive, you've now received your

extra 3 GB of storage." OneDrive comes by default with 7 GB of storage space, so the extra 3 GB clearly come in handy, especially for users who are planning to store all their camera photos in the cloud. To read more click **HERE**