The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
7+10 February 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

February 6, Help Net Security – (International) **Insecure file sharing puts corporate data at risk.** Globalscape released the results of a survey of over 500 corporate professionals and found that in the past 12 months, 63 percent of employees used personal email to send sensitive documents, and that employees frequently used potentially insecure consumer cloud services and sites to store sensitive information, among other findings. Source: http://www.net-security.org/secworld.php?id=16318

February 7, Softpedia – (National) **HVAC company makes statement on Target data breach.** Fazio Mechanical Services confirmed that attackers used a data connection with Target used for billing, project management, and contract submission to breach Target's systems and steal large amounts of customer payment information. Source: http://news.softpedia.com/news/HVAC-Company-Makes-Statement-on-Target-Data-Breach-424941.shtml

February 6, Salisbury Daily Times – (Delaware; Pennsylvania) **Beebe Healthcare says 1,900 patients affected by security incident.** Beebe Healthcare terminated a Beebe Physician Network temporary contractor in Delaware after learning they had access to about 1,900 patients' personal information and had previously been arrested in connection with identity theft incidents in Pennsylvania. The organization notified the patients and do not believe any information was removed or improperly accessed. Source: http://www.delmarvanow.com/article/20140206/NEWS/302060044

February 6, KXLT 47 Rochester – (National) **OMC: No evidence data breach was initiated internally.** Officials at Olmstead Medical Center in Rochester verified a breach February 5 in which employee data was accessed without authorization. The medical center continues to investigate what specific data was illegally accessed, which may have included Federal W-2 statements. Source: http://www.myfox47.com/story/24657134/2014/02/06/omc-no-evidence-breach-of-data-was-initiated-internally

February 7, Softpedia – (International) **Cybercriminals hijack router DNS settings to lure users to fake banking websites.** Researchers at Poland's Computer Emergency Response Team (CERT Polska) identified an attack that uses vulnerabilities in home routers to redirect users to fake banking Web sites. The attack hijacks DNS settings and then redirects users to malicious Web sites that mimic legitimate banking sites. Source: http://news.softpedia.com/news/Cybercriminals-Hijack-Router-DNS-Settings-to-Lure-Users-to-Fake-Banking-Websites-424920.shtml

February 7, Help Net Security – (International) **Facebook bug prevents revocation of app permissions.** Developers at software vendor MyPermissions identified a vulnerability in Facebook's mobile app that can be exploited to make it impossible for users to revoke permissions given to Facebook apps. The vulnerability was reported to Facebook and a solution is being developed. Source: http://www.net-security.org/secworld.php?id=16331

Sochi security forbids journalists to use private Wi-Fi

Heise Security, 10 Feb 2014: The Winter Olympics in Sochi are under way, and we have already written about the cyber risks awaiting visitors and viewers. But what about the ones awaiting the visiting media representatives? Yahoo! Sports' reporter Charles Robinson has shared a few interesting tweets last week that depicted an individual monitoring laptop computers to ensure they were not using WiFi (later determined to be a member of Russia's "spectrum management team", which seizes PC users caught using WiFi). There's no explanation of why the use of private wireless access points is forbidden. At the Main Media Center in Sochi, the journalist has the option to use the slower free Wi-Fi or the paid higher speed one. Also, the Olympics at Sochi are the first time that the media has been offered free Wi-Fi access. But, as the Guardian reported, "major amendments have been made to telephone and Wi-Fi networks in the Black Sea resort to ensure extensive and all-permeating monitoring and filtering of all traffic, using Sorm, Russia's system for intercepting phone and internet communications," so naturally there's speculation on whether this move is to prevent the media using un-monitored Wi-Fi networks. Whatever the underlying reason, journalists found using private WACs are apparently expelled from the room (possibly even from the Media Center?). To read more click **HERE**

Account details of 27,000 Barclays customers stolen, sold to brokers

Heise Security, 10 Feb 2014: (In)famous UK-based multinational bank Barclays has been hit this Friday with claims that someone has stolen personal and financial information of some 27,000 of its customers and has been selling it to City traders. The revelation was published by The Mail on Sunday, and is based partial information - a sample of the stolen files - provided by a whistleblower that wants the affected customers to be warned and wary of cold calls made by unscrupulous traders. The stolen records apparently contain the customers' name, date of birth, national insurance number, address, phone number, passport number, employment status, occupation, earnings, extensive financial status information as well as a summary of their attitude to financial risk, their financial goals, and even some information about their health and private interests. The whistleblower - a former commodity broker - says that each record was priced around £50 ($82), and that many traders have opted to buy some of the files. The whistleblower became aware of the existence of the files in September 2013 when he was asked by the boss of the brokerage firm he was working for to sell the leads to other brokerages for £8 per file, as they were "done" with them. Apparently, this particular firm started using these files on December 2012, so the breach is definitely old. It is still unclear how the records were stolen - chances are it's an insider - and the bank has initiated an investigation after The Mail published the report. Still, it seems unbelievable that the bank hasn't suspected anything for such a long time. Whatever the case may be, they are investigating now, and they have contacted the Information Commissioner and other regulators immediately upon being appraised of the situation. Initial results indicate that the stole information belongs to customers linked to the bank's Financial Planning business that was shut down in 2011. To read more click **HERE**

Mobility is the weakest security link

Heise Security, 7 Feb 2014: Surveying more than 750 security decision makers and practitioners, a CyberEdge Group report found that more than 60 percent had been breached in 2013 with a quarter of all participants citing a lack of employer investment in adequate defenses. Their key findings include:

- Concern for mobile devices. Participants were asked to rate — on a scale of 1 to 5, with 5 being highest — their organization's ability to defend cyber threats across nine IT domains. Mobile devices (2.77) received the lowest marks, followed by laptops (2.92) and social media applications (2.93). Virtual servers (3.64) and physical servers (3.63) were deemed most secure.
- The BYOD invasion. By 2016, 77 percent of responding organizations indicate they'll have BYOD policies in place. 31 percent have already implemented BYOD policies, 26 percent will follow within 12 months, and another 20 percent will follow within two years.

- Inadequate security investments. Although 89 percent of respondents' IT security budgets are rising (48 percent) or holding steady (41 percent), one in four doubts whether their employer has invested adequately in cyber threat defenses.
- Improved security or wishful thinking? Although 60 percent of respondents confessed to being affected by a successful cyber attack in 2013, only 40 percent expect to fall victim again in 2014.
- Malware and phishing causing headaches. Of eight designated categories of cyber threats, malware and phishing/spear-phishing are top of mind and pose the greatest threat to responding organizations. Denial-of-service (DoS) attacks are of least concern.
- Ignorance is bliss. Less than half (48 percent) of responding organizations conduct full-network active vulnerability scans more frequently than once per quarter, while 21 percent only conduct them annually.
- Dissatisfaction with endpoint defenses. Over half of respondents indicated their intent to evaluate alternative endpoint anti-malware solutions to either augment (34 percent) or replace (22 percent) their existing endpoint protection software.
- Careless employees are to blame. When asked which factors inhibit IT security organizations from adequately defending cyber threats, "low security awareness among employees" was most commonly cited, just ahead of "lack of budget."

To read more click **HERE**

Hackers breach Comcast's mail servers

Heise Security, 6 Feb 2014: After successfully targeting Bell Canada and leaking customer information, hacker collective NullCrew has apparently breached mail servers belonging to Comcast, the largest ISP in the US. They claim to have exploited a local file inclusion (LFI) vulnerability in Zimbra, a groupware email server and web client used on 34 Comcast mail servers, to access them and their content. To prove their "conquest", they linked to a Pastebin post containing a list of the servers, and the exploit code they apparently used in the attack. Databreaches.net reports that the post didn't include customer information, although one of the attackers implied that they have gotten their hands on a password database. Comcast has yet to comment on the claims, but they shut down their mail servers for the time being. To read more click **HERE**

Every two seconds there's a new victim of identity fraud

Heise Security, 6 Feb 2014: Javelin Strategy & Research reports an increase of more than 500,000 fraud victims to 13.1 million people in 2013. Account takeover fraud hit a new record in incidence for the second year in a row and accounted for 28 percent of all identity fraud. Additionally, fraudsters increasingly turned to eBay, PayPal and Amazon with the stolen information to make purchases. In 2013, data breaches became more damaging, with one in three people who received a data breach notification letter becoming an identity fraud victim. Encouragingly, the amount criminals stole decreased by $3 billion to $18 billion, reflecting more aggressive actions from financial institutions, identity theft protection providers and consumers. Identity fraud is defined as the unauthorized use of another person's personal information to achieve illicit financial gain. Identity fraud can range from simply using a stolen payment card account, to making a fraudulent purchase, to taking control of existing accounts or opening new accounts, including mobile phone or utility services. In October 2013, Javelin Strategy & Research conducted an address-based survey of 5,634 U.S. consumers to identify important findings about the impact of fraud, uncover areas of progress and identify areas in which consumers must exercise continued vigilance. More victims, less stolen - The number of identity fraud incidents increased by 500,000 consumers over the past year, while the dollar amount stolen decreased to $18 billion, significantly lower than the all-time high of $48 billion in 2004. Individuals between 35-44 were at greatest risk. When successful, fraudsters are now more than three times as likely to use the money stolen to buy prepaid or gift cards to make fraudulent purchases. Types of fraud changed - account takeover rose dramatically — Criminals are changing behavior to exploit vulnerabilities. Most tellingly, account takeover hit a new record in incidence for the second year in a row and accounted for 28 percent of identity fraud losses. Account takeovers for utilities and mobile phone fraud nearly tripled, as fraudsters add new properties to victims' utility accounts and run up unauthorized charges using "premium" texting services. Consumers that are a victim of account takeover tend to start paying bills online to improve security. Data breaches are the greatest risk factor for identity fraud - In 2013, one in three consumers who received notification of a data breach became a victim of fraud. This is up from one in four in 2012. Forty-six percent of consumers with breached debit card in 2013 became fraud victims in the same year, compared to only 16 percent of consumers with a Social Security number breached. Identity fraud is more than just credit card fraud - Specifically, non-card fraud saw a rapid rise in 2013. The number of non-card fraud victims nearly tripled and it accounted for $5 billion in fraud. To read more click **HERE**

Pakistan Exchange to Probe Data Leak after Staff Members Removed
Heise Security, 10 Feb 2014

Pakistan's Karachi Stock Exchange formed a team to investigate possible data leaks and removed some employees for acting inappropriately. "The management received information in August 2013 alleging that in 2008 there was misappropriation in the purchase of some IT hardware and some IT personnel had access to KSE's IT system during that period," according to a statement issued by the exchange dated Feb. 7. The management "removed from service several IT staff as they were deemed to have acted inappropriately." The bourse put together a group of outside forensic specialists and senior exchange management to probe whether any data was leaked amid vulnerabilities related to the bourse's computer network as identified by consultants, according to the statement. The KSE 100 Index (KSE100) fell 1.6 percent at 1:27 p.m. in Karachi, heading for its biggest loss in four months. Reuters reported last week the exchange is investigating whether staff profited from years of unauthorized access to real time trading data. The KSE 100 has surged about 380 percent in the past five years as rising consumer spending boosted earnings in an economy hurt by power blackouts and a Taliban insurgency. Prime Minister Nawaz Sharif, who came to power in June, is moving to overhaul the economy through share sales of state-run companies and improved infrastructure. A separate review of the IT department will be finished by the end of this month, the exchange said, while a report produced by consultants in December 2013 didn't find any evidence of leaked trading data. To read more click **HERE**

Cybercriminals Use CryptoLocker to Encrypt Files of US Law Firm
Heise Security, 10 Feb 2014: A law firm in Charlotte, North Carolina, has admitted falling victim to a cyberattack that leveraged the notorious piece of ransomware called CryptoLocker. According to WSOCTV, the attackers infected one of the company's servers after sending out a fake voicemail notification that had the malware attached to it. After the law firm's IT department failed to recover the files, it agreed to pay the $300 (€220) to get them back. However, at that point, it was already too late. The company's representatives say they've lost access to thousands of legal documents, but no confidential information appears to have been stolen. Experts recommend against paying the ransom money, but many organizations, particularly small businesses, have often given in to the extortionists. A police department in the US has admitted paying $750 (€555) to recover the files. CryptoLocker victims are instructed to pay the ransom in 72 hours. After that, they can still recover their files by using a specialized service, but the amount of money they have to pay is much higher. To read more click **HERE**

How to Reset the Password on Any Windows Version, Including 8.1, From Linux
SoftPedia, 8 Feb 2014: If you have a Windows operating system and you find yourself locked out, Linux is there for the rescue with a very handy tool, ntpasswd. ntpasswd can be described as an "Offline NT Password & Registry Editor" and it's a tool that can be used to reset the password of any user that has a valid account on a Windows system. The beauty of this tool is that it works on any system from NT3.5 on up, even the latest Windows 8.1. Its developer says it will also

work on 64-bit architectures and the server versions (such 2003, 2008, 2012). This is how it works, according to it's maker: “Windows stores its user information, including crypted versions of the passwords, in a file called 'sam', usually found in \windows\system32\config. This file is a part of the registry, in a binary format previously undocumented, and not easily accessible. But thanks to a German(?) named B.D, I've now made a program that understands the registry.” For the most part the system is fully automated, but you need to read the documentation very carefully as it can also ruin your system. The ntpassw tool is provided under the form of an image, which can be written on a CD or USB. If this does work, the developer also provides other means of running this tool, from another LiveCD, like Ubuntu. To read more click **HERE**

Three Home Depot HR Employees Arrested for Stealing Co-Workers’ Information
SoftPedia, 8 Feb 2014: Earlier this week, three individuals working in the human resources department of Home Depot’s corporate headquarters in Atlanta were arrested and charged with stealing their co-workers’ personal information and using it for fraudulent credit cards. Claudette Grimes and her daughter, Lakisha Grimes, and Paulette Shorter are the suspects. They’ve all been released on bail, WSBTV reports. Home Depot representatives say the trio’s illegal activities had been uncovered after someone from the company’s security department noticed that an email sent by Claudette Grimes from her work account contained the details of over 300 employees. The incident was reported to the US Secret Service. The information included social security numbers and birth dates. The 300 individuals have been notified and Home Depot is offering them free credit monitoring services. The company says between 10,000 and 20,000 employees’ information might have been exposed. Home Depot customers are not impacted, because the HR employees didn’t have access to their information. To read more click **HERE**

Russia Bans Bitcoin
SoftPedia, 8 Feb 2014: Russia has completely banned Bitcoin, the cryptocurrency that’s taken the world by storm. The Central Bank of Russia has reiterated that the official currency is the Ruble and that Bitcoin is viewed as a money substitute, which is why the digital currency is now officially banned. The decision comes as a result of the many cases when Bitcoin was used for money laundering and other criminal activities. Of course, this hasn’t been proven thus far in a court of law and these are mere allegations at this point, but chances are authorities are right about this topic. However, it’s going to be rather difficult for Russian users of Bitcoin to comply to the new laws overnight. Given the fact that Bitcoin is a free currency and doesn’t really rely on any physical institution in Russia, users may be able to fly under the radar. To read more click **HERE**

Tesla Motors Wants to Make Sure Its Cars Are Secure, Hires Hacker
SoftPedia, 8 Feb 2014: Kristin Paget (formerly known as Chris Paget), the world-class security expert hired by Apple in December 2012, has announced that she has joined Tesla Motors. Paget hasn’t revealed too much about her role at the electric car maker, but it will probably involve “securing things.” She has told Re/code that she starts on Monday at the company’s headquarters in Palo Alto, California. Commenting on Tesla’s decision to hire Paget, Malwarebytes’ Jean Taggart said, “It is refreshing to see a company like Tesla address the potential security risks so early in the game, where the general sentiment coming from the security industry is that we won’t have proper security in place until after some catastrophic event occurs.” To read more click **HERE**

Bank of America Customers Targeted in Massive Bredo Malware Distribution Campaign
SoftPedia, 7 Feb 2014: Security researchers at AppRiver have spotted an interesting malware distribution campaign that leverages a massive volume of traffic in an effort to evade filtering engines. The attack is aimed at Bank of America customers and, at its peak, AppRiver’s data center recorded 10 to 12 times the normal amount of traffic. Cybercriminals are sending out fake Bank of America emails that carry a piece of malware of the Bredo family. This threat is designed to steal information, including banking data, from infected devices. The Trojan is also capable of downloading other

malicious elements onto affected computers. At the time of the attack, the malware sample analyzed by experts was identified by only 11 antivirus engines. AppRiver says that it has managed to block the spam messages, but this incident shows that cybercriminals are increasingly turning to this method to beat filtering engines. To read more click **HERE**