The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

13 January 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

January 10, Bloomberg News – (National) **Target raises estimate of customers hit by breach.** Target Corp., stated January 10 that names, email addresses, and home addresses for up to 70 million customers were also stolen during a breach of its systems that compromised the payment card information of around 40 million customers. Source: http://www.bloomberg.com/news/2014-01-10/target-raises-estimate-of-customers-hit-by-breach.html

January 10, Associated Press – (Georgia) **Hospital system probing data breach.** Officials at Phoebe Putney Hospital in Albany, Georgia, notified more than 6,700 patients after a computer that may have held their unencrypted personal information went missing in November 2013. The hospital continues to investigate the incident. Source: http://www.11alive.com/news/article/318436/3/Hospital-system-probing-data-breach

January 10, Help Net Security – (International) **Sefnit trojan endangers users even after removal.** Microsoft researchers warned that computers previously infected with the Mevade botnet malware that used a The Onion Router (TOR) connection for malicious uses in 2013 may be vulnerable to future attacks due to the version of TOR that came with the malware not self-updating. Source: http://www.net-security.org/malware_news.php?id=2673

January 10, Softpedia – (International) **There are still at least 22,000 devices infected with Flashback Mac malware.** Researchers at Intego reported finding at least 22,000 Macs that are still infected with the Flashback information stealing trojan. Intego currently runs sinkhole servers for the malware but warned that it is possible that cybercriminals could regain control of command and control servers in the future. Source: http://news.softpedia.com/news/There-Are-Still-at-Least-22-000-Devices-Infected-with-Flashback-Mac-Malware-415511.shtml

January 9, IDG News Service – (International) **Yahoo malvertising attack linked to larger malware scheme.** Research by Cisco Systems found that a recent cyberattack that served malicious ads to European users of Yahoo appears to be connected to a traffic-pushing scheme based in Ukraine. Source: http://www.networkworld.com/news/2014/011014-yahoo-malvertising-attack-linked-to-277587.html

Man Admits Hijacking YouTube Channels, Hacking AOL CEO's Email Account
SoftPedia, 13 Jan 2014: A 28-year-old man from Maryland, US, has pleaded guilty to hijacking YouTube accounts in an effort to make a profit via the video sharing site's ad service. He has also admitted hacking the email account of AOL's CEO. According to the Washington Post, Matthew A. Buchanan made almost $56,000 by abusing hijacked YouTube accounts. Buchanan's accomplice, John T. Hoang Jr., wrote a piece of software designed to scan YouTube for popular channels that weren't using Google's Adsense service to make money through advertisements. They're said to have identified 200,000 Google accounts, some of which they hacked by abusing the password reset process. Court documents show that the suspects

exploited a flaw in the process to obtain the victim's email address. Then, they used special software for cracking passwords, or guessed the answers to the security questions in order to hijack the accounts. Another clever method utilized by the cybercriminals included registering email accounts such as dog@yahoo.com. When registering accounts, many users will enter such email addresses as secondary addresses because they think they don't exist, and they don't want to go through the trouble of registering a secondary email. However, some of these apparently non-existent addresses do exist, and some of them were controlled by Buchanan and Hoang. The men used these accounts to have temporary passwords sent to them. The scheme lasted between June 2012 and September 2013. As far as the AOL hacking is concerned, Buchanan admitted breaching the accounts of several employees, including the company's CEO, by exploiting a vulnerability in the email service. He said he did it as part of a hobby that involved looking for security issues on the Internet. Buchanan will be sentenced on March 28, 2014. He faces five years in prison for his crimes. To read more click **HERE**

Oracle to Patch 36 Java Vulnerabilities with January 2014 CPU
SoftPedia, 14 Jan 2014: On Tuesday, Oracle will release its Critical Patch Update (CPU) for January 2014. A total of 144 security holes will be addressed, including 36 that impact Java. The list of products affected by the flaws includes Database, Fusion Middleware, Enterprise Data Quality, Forms and Reports, Portal, Outside in Technology, GlassFish Server, HTTP Server, Identity Manager, Internet Directory, iPlanet, Reports Developer, VM VirtualBox, MySQL Enterprise Monitor and Server, Siebel, Solaris, E-Business Suite and others. Some of the vulnerabilities fixed with this update impact multiple pieces of software. As far as Java is concerned, 34 of the 36 security holes addressed by Oracle with the January 2014 CPU can be exploited remotely and without authentication. The affected Java SE components are Java SE, Java SE Embedded, JavaFX and JRockit. For additional details on the January 2014 CPU, check out Oracle's advisory. To read more click **HERE**

The Official Microsoft Blog Hacked by Syrian Electronic Army
SoftPedia, 12 Jan 2014: As I told you yesterday, the Syrian Electronic Army hacked the official Microsoft News Twitter account and posted several anti-Microsoft messages as a protest against Redmond's alleged involvement in NSA's spying programs. It turns out, however, that the SEA has also managed to break into the official Microsoft blog and post a big message reading "Hacked by Syrian Electronic Army," while also linking to the its tweets published with the hacked @MSFTNews account. Again, the software giant reacted pretty fast and removed all posts, so the blog is up and running right now with no signs of hacks. According to some leaked emails that reached the web soon after the hack, Microsoft has changed the passwords to all its blogs and social accounts, in an attempt to prevent further attacks from happening. The company says that no user information has been compromised during the attack, so users are all safe. To read more click **HERE**

MIT Subdomain Hacked by Anonymous One Year After Aaron Swartz Committed Suicide
SoftPedia, 11 Jan 2014: Shortly after Reddit cofounder and activist Aaron Swartz committed suicide on January 11, 2013, Anonymous hackers defaced the website of the Massachusetts Institute of Technology (MIT). Now, one year after his death, hacktivists have targeted MIT's website once again. Hackers have defaced the subdomain used by MIT for the Cogeneration Project (cogen.mit.edu). On the website, the following message has been posted, "Remember The Day We Fight Back, Remember. We Never Forget, We Never Surrender, Expect Us." Security expert Janne Ahlberg says it's possible that the hackers leveraged an SQL Injection vulnerability to breach the website. The attack is part of Operation Last Resort, the campaign initiated shortly after Swartz's death. The message from the hackers contains a link to "The Day We Fight Back," a website that militates against mass surveillance. At the time of writing, the MIT subdomain is still defaced. Several high-profile websites were hacked as part of OpLastResort in the past, including the Federal Reserve, the Sentencing Commission, the National Association of Federal Agents, and the Department of State. In case you're not very familiar with Aaron Swartz's story and you're wondering why Anonymous has targeted MIT, it's because the

organization's actions led to the activist being prosecuted, which ultimately led to him committing suicide. Swartz was accused of illegally downloading a large number of documents from the digital repository JSTOR through MIT's networks. MIT security caught him on camera while downloading data with the aid of a laptop connected to a switch in a wiring closet. The video has recently been provided by authorities to Kevin Poulsen, the man who filed a lawsuit against the US government in an effort to obtain all the documents the Secret Service had on Swartz. After Swartz's death, US officials have been trying to make modifications to the controversial Computer Fraud and Abuse Act (CFAA). To read more click **HERE**

Hackers Steal Payment Card Data from Systems of Neiman Marcus

SoftPedia, 11 Jan 2014: The systems of Neiman Marcus, a Dallas-based retailer that specializes in luxury goods, have been hacked. As a result of the breach, customer payment card information has been compromised. Brian Krebs says that he learned of the breach earlier this week from his sources in the financial industry. Apparently, the stolen information is already being abused for fraudulent charges. Neiman Marcus representatives have confirmed for Krebs that their systems have been breached. They learned of the breach in mid-December after being notified by their credit card processor. So far, the company doesn't know how the cybercriminals gained access to the payment card information, and it's uncertain for how long they've had access to their systems. Currently, there's no evidence that individuals who made purchases on Neiman Marcus' website are impacted. "We informed federal law enforcement agencies and are working actively with the U.S. Secret Service, the payment brands, our credit card processor, a leading investigations, intelligence and risk management firm, and a leading forensics firm to investigate the situation," Neiman Marcus spokesperson Ginger Reeder explained. Neiman Marcus is not the only retailer targeted by cybercriminals last year. Target also suffered a massive data breach in which customer payment cards have been compromised. Initially, the company said around 40 million people were affected. However, on Friday, it revealed that the names, addresses, email addresses or phone numbers of 70 million customers had been obtained by the attackers. In Target's case, it's uncertain who is behind the attack, but Krebs has identified one Ukrainian who appears to be responsible for selling the stolen card data on the underground market. It's uncertain if he's directly involved in the breach, but he does have some connection to it since he had offered Krebs $10,000 (€7,300) not to run his story. To read more click **HERE**

Google Helped Fix 1,000 Bugs in FFmpeg Over Two Years

SoftPedia, 11 Jan 2014: In the past couple of years, Google has helped fix over 1,000 bugs in FFmpeg, the company announced. Google has been using its data centers for fuzzing, which is a large scale automated testing called fault injection performed by data centers. FFmpeg is the free software project that is used to produce libraries and programs for a wide range of purposes, including streaming audio and video, recording and converting data. "At Google, security is a top priority - not only for our own products, but across the entire Internet. That's why members of the Google Security Team and other Googlers frequently perform audits of software and report the resulting findings to the respective vendors or maintainers, as shown in the official "Vulnerabilities - Application Security" list," Google's Mateusz Jurczyk and Gynvael Coldwind wrote in a blog post. Numerous apps use FFmpeg, including Google's own Chrome, but also popular media player VLC. According to the company, in the past two years, over 1,000 bugs were fixed with their help, while another 400 bugs were fixed alongside developers of Libav. "We are continuously improving our corpus and fuzzing methods and will continue to work with both FFmpeg and Libav to ensure the highest quality of the software as used by millions of users behind multiple media players. Until we can declare both projects "fuzz clean" we recommend that people refrain from using either of the two projects to process untrusted media files. You can also use privilege separation on your PC or production environment when absolutely required," the announcement reads. The two information security engineers from Google who were in charge of the blog post, detailed the entire process they've gone through in the past couple of years, including how they first started out giving a helping hand to the FFmpeg team. To read more click **HERE**

Fake "Critical browser update" warnings lead to malware
Heise Security, 10 Jan 2014: If you have manually updated your browser in the last week or so, think back on how you did it. Did you look for the update yourself, or did you download one after being faced with a warning saying you should pick up a "critical update"? If it's the latter, and if you are living in the UK, chances are you fell for the latest malware delivery campaign that was started just before New Year's Eve. You probably visited a free movie streaming or media site, and a malicious ad redirected you to another website. "The website, which is hosted in the Ukraine, uses a dual hybrid Web server setup by Apache and Nginx, with the latter identifying the victim's browser and performing a redirect," Symantec researchers explained in a recent blog post. On the site on which you ended up, a warning using a template corresponding to your browser type was shown, and you were offered the update for download. Had you refused, a JavaScript loop would have forced you to stay on the site by making it impossible to close your browser unless you performed an extensive series of repetitive clicks. If you have downloaded and run the update, you should know that your computer has been likely been infected with the information-stealing Shylock Trojan, and you should use an AV solution to disinfect your machine. To read more click **HERE**

Fake Target breach notification leads to phishing and complex scams
Heise Security, 13 Jan 2014: The extensive Target breach has resounded far and wide in US media, and its customers should worry about their personal or credit card information being misused. After the initial breach revelation in late December, the company has started sending out breach notices to potentially affected customers, and continued to do so in the wake of the discovery of additional compromised information. But cyber scammers have also started send out notifications in Target's name, trying to trick users into sharing their personal information, as well as to complete online surveys. According to the number of these spam emails collected by Malcovery in the last few days, the campaign is not (yet) massive. The email in question tries to get the victims' attention but proclaiming "Alert to Target Shoppers - your identity is at risk" in the subject line. Currently, the email is sent from a Yahoo email address that obviously has nothing to do with Target. But the worrisome content of the email might nevertheless spur some users to click on the offered links. This email is not a real, straightforward phishing email. Users who follow the links are taken via a series of redirects to a page with a survey and offering a $1000 shopping voucher Sears/JCPenney/Kohl's/Macy's as an incentive. But once that survey is completed, they are redirected to new surveys on different pages run on systems by different ad companies. Among other things, the victims are instructed to answer questions that can be used to create a pretty accurate idea of their shopping activities, which will then be directly tied to their real-world identity, as the victims are then urged to enter their name, address, phone number, email address, date of birth, etc. Once that task is over, there are still a lot of personal questions to be answered. Then questions about employment, education and their health are trotted out, and all the while the scammers dangle the reward (which has not turned to a $150 Walmart gift card) before the users. Then another set of surveys is trotted out. And then the victim is required to download an add-on (a ShopAtHome.com Toolbar) and make it its default search provider and default new tab. Finally, they are told they must buy a set of knives or sign up for a credit report service, and then to buy more things. The complexity of this scam is astounding. Unfortunately, there are always - always! – more than enough inexperienced Internet users who fall for it, and make it worth while for the scammers. To read more click **HERE**

Senior managers are the worst information security offenders
Heise Security, 8 Jan 2014: As companies look for solutions to protect the integrity of their networks, data centers, and computer systems, an unexpected threat is lurking under the surface—senior management. According to a new survey, 87% of senior managers frequently or occasionally send work materials to a personal email or cloud account to work remotely, putting that information at a much higher risk of being breached. Released by global investigations, intelligence, and risk services company Stroz Friedberg, the survey also found that 58% of senior management reported having accidentally sent the wrong person sensitive information, compared to just 25% of workers overall. Corporate managers also put their companies at risk of intellectual property loss if and when they depart the company. Fifty-one

percent of senior management and 37% of mid-level management admit to taking job-related emails, files, or materials with them when they have left past employers. Only one-fifth of lower ranking employees have done so. “Insiders are by far the biggest risk to the security of a company’s sensitive information, whether it’s a careless executive or a disgruntled employee. When information is compromised, a company’s reputation, customer base, and share price may suffer,” said Michael Patsalos-Fox, CEO of Stroz Friedberg. “Our inaugural information security survey demonstrates that companies need to address high-risk security behaviors within the workplace at all levels with a proactive risk mitigation plan.” The national survey of 764 information workers explored the state of information security in U.S. businesses and surveyed respondents online regarding their thoughts on the biggest information security threats, cyber security risk mitigation, company security vulnerabilities, and the state of corporate America’s response to cyber threats. The survey found that senior leaders in general believe their own security efforts are inadequate:

- Nearly half (45%) of senior management acknowledge that the C-suite and senior leadership themselves are responsible for protecting their companies against cyber-attacks.
- Yet, 52% of this same group indicated they are falling down on the job, rating corporate America’s ability to respond to cyber-threats at a “C” grade or lower.
- Rank-and-file workers differ in their opinions about cyber security accountability, with 54% of those respondents saying IT professionals are responsible for putting the right safeguards in place.

Employees admit fears regarding the security of their personal information at work, with 73% of respondents reporting concern that a hacker could gain access to their company’s network and steal sensitive, personal records such as their Social Security number, birthday, or home address. This worry perhaps reflects their thoughts regarding how well businesses in general are responding to cyber threats and in safeguarding sensitive or proprietary information; more than 60% of employees gave American businesses a “C” or lower when asked to grade their performance on this critical task. BYOD and the use of personal online accounts have become prevalent in American businesses, as workers use their personal smartphones, tablets, and preferred cloud providers to stay productive while at work and out of the office. This is opening the door for businesses to encounter new and emerging threats from hackers, malware, and viruses. A lack of corporate communication and training is also a likely culprit to explain these behaviors:

- Only 35% of respondents reported receiving regular training and communications on mobile device security from their employers
- Thirty-seven percent of employees received training on social media use
- Employees reported information sharing training just 42% of the time.

The complete survey is available **here**. To read more click **HERE**