The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
22 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 17, Associated Press – (Puerto Rico) **Personal information of Puerto Rico doctors stolen.** The president of Puerto Rico's Association of Surgeons stated that the association's electronic system was recently hacked and the personal information of all medical doctors licensed to practice on the island was stolen. The doctors have also been receiving harassing emails. Source: http://www.washingtonpost.com/world/the_americas/personal-information-of-puerto-rico-doctors-stolen/2014/01/17/e8354b96-7f9b-11e3-97d3-b9925ce2c57b_story.html

January 21, Threatpost – (International) **Cutwail-like spambot hides malicious activity in its traffic.** Researchers at Dell SonicWALL identified a new spam botnet dubbed Wigon.PH_44 being served on compromised Web sites hosted on the WordPress platform that uses large amounts of HTTP POST and GET requests in order to disguise the true nature of its traffic. Source: http://threatpost.com/cutwail-like-spambot-hides-malicious-activity-in-its-traffic/103744

January 21, Softpedia – (International) **Android malware disguised as security update steals SMSs and intercepts phone calls.** FireEye researchers identified six versions of a new Android malware dubbed Android.HeHe that can intercept SMS messages and phone calls from numbers specified in a file. The malware is being distributed disguised as a security update for Android. Source: http://news.softpedia.com/news/Android-Malware-Disguised-as-Security-Update-Steals-SMSs-and-Intercepts-Phone-Calls-419230.shtml

January 21, The Register – (International) **Hacker breaks into ThrustVPS, launches phishing attack from firm's own servers.** Virtual private server company ThrustVPS stated that they were the victim of a phishing attack that compromised their systems and allowed an attacker to upload a php shell and mailer script, which caused phishing emails to be sent from the company's servers. Source: http://www.theregister.co.uk/2014/01/21/thrustvps_penetrated_by_phishing_attack/

January 20, The Register – (International) **Google pulls Chrome extensions after new owners subvert web tools.** Google pulled at least two extensions for its Chrome browser from the company's online store after a researcher found that spammers and other malicious actors bought the software from developers and then added advertising or other unwanted components to updates for the extensions. Source: http://www.theregister.co.uk/2014/01/20/google_pulls_chrome_extensions_after_new_owners_subvert_web_tools/

January 20, Threatpost – (International) **Starbucks fixes vulnerable iOS app, geolocation issue persists.** Starbucks issued a patch for its iOS app that was found to contain user names and passwords in plain text. Source: http://threatpost.com/starbucks-fixes-vulnerable-ios-app-geolocation-issue-persists/103730

January 18, Softpedia – (International) **Android vulnerability can be exploited to capture data of VPN users.** Researchers at Ben Gurion University identified a vulnerability in Android that could be used to bypass active virtual private network (VPN) configurations in order to intercept secure communications. The researchers released a proof-of-concept for the vulnerability. Source: http://news.softpedia.com/news/Android-Vulnerability-Can-Be-Exploited-to-Capture-Data-of-VPN-Users-418314.shtml

Did you get an email from Target? What you need to know
CNN Money, 21 Jan 2014: Are you one of the roughly 70 million people who got an email from Target last week about the store's mega security breach? If so, be careful. Target did indeed do a blast to customers to offer one year of free credit monitoring. The problem is scammers are also on the prowl and are sending out similar emails. Target even says it has identified and stopped at least 12 scams preying on consumers via email, Facebook and other outlets. The Target emails went to customers whose personal information was in the Target database. Cyber thieves penetrated the records during the holiday shopping season breach discovered last month and stole info like names, phone numbers and email addresses. The full extent of the hacking is still under investigation. In the meantime, here's what to do if you see an email from Target pop up in your inbox. If you've already opened the email: Target has posted a copy of the email it sent out online. So go here to make sure the email you opened, the address it came from, and the link you clicked all matches up. If it doesn't match, and especially if you clicked a link to an external website and entered personal information, you need to take action quickly, says Credit.com Chairman Adam Levin, who specializes in privacy and identity theft. First, get a copy of your credit report, check your bank and credit card activity on a daily basis and call the credit reporting agencies to tell them what happened. You can ask to have a fraud alert placed on your account, meaning it will be flagged to lenders if someone attempts to open credit in your name. If you're really worried, you can request a credit freeze, which prohibits any credit from being extended under your name. But that's a big step because you will have to go through the process of undoing this whenever you need credit again. If you entered a credit card or debit card number, reach out to those institutions to warn them of potential fraud as well. If you haven't opened the email: To avoid any chance of a virus or of falling prey to a potential scam, Levin recommends going directly to Target's website to view the letter you believe has landed in your inbox -- since even opening a fraudulent email could lead malware to be installed on your computer. And if you do open the email, don't click on any links. You can also visit creditmonitoring.target.com directly to enroll in the free credit monitoring Target is offering. Once there, you will have to enter your email address and will be sent another email within 72 hours with a unique activation code to use in order to sign up for the service. The subject will mention the activation code. The retailer emphasizes that it will never email a consumer and ask for personal information like a Social Security number or credit card information. To read more click **HERE**

13 People Indicted for Role in Gas Station Card Skimming Operation
SoftPedia, 22 Jan 2014 New York authorities have indicted a total of 13 individuals suspected of stealing payment card information by installing skimming devices at gas station pumps located all across the southern part of the US. The stolen information has been used to withdraw over $2 million (€1.5 million) from banks and ATMs in Manhattan. According to the New York District Attorney's Office, the lead defendants are Garegin Spartalyan, 40, Aram Martirosian, 34, Hayk Dzhandzhapanyan, 40, And Davit Kudugulyan, 42. They were arrested in March 2013. They've been charged with money laundering, grand larceny, criminal possession of a forgery device, criminal possession of forged instruments, and criminal possession of stolen property. The other defendants have been charged with two counts of money laundering in the second degree or money laundering in the third degree. The suspects are said to have installed credit card skimming devices at Raceway and Racetrac gas stations in South Carolina, Texas and Georgia. The skimmers recorded not only card numbers, but also PINs. What's interesting about this scheme is that the crooks didn't need to gain physical access to the devices in order to retrieve the stolen information. That's because the data could be obtained via Bluetooth. Authorities believe the lead defendants are responsible for encoding the stolen data onto blank cards.

The money had been withdrawn from ATMs in Manhattan and deposited into bank accounts. The operation took place between March 2012 and March 2013. Each of the fraudulent transactions was kept under $10,000 (€7,300) in order to avoid raising any suspicion. "By using skimming devices planted inside gas station pumps, these defendants are accused of fueling the fastest growing crime in the country," stated Manhattan District Attorney Cyrus R. Vance, Jr. "Cybercriminals and identity thieves are not limited to any geographic region, working throughout the world behind computers. In this case, the defendants are charged with stealing personal identifying information from victims in southern states, used forged bank cards on the East Coast, and withdrew stolen proceeds on the West Coast." To read more click **HERE**

Russian Man Admits Developing Malware Used in Target Attack
SoftPedia, 21 Jan 2014: Last week, InterCrawler revealed the identity of a 17-year-old teen from Russia who was allegedly responsible for the creation of the malware used in the Target attack. After further analysis, the company has determined that the teen, Sergey Taraspov, is in charge for technical support and that the real developer is actually one Rinat Shabayev. In an interview with Russian publication LifeNews, Shabayev, who lives in the city of Saratov, has admitted developing the application that has been dubbed BlackPOS and Kaptoxa. However, the 23-year-old says that his creation is not intended for criminal purposes. He claims to have written the program for security testing. On the other hand, he does admit that it can be used for malicious purposes. Shabayev has allegedly developed the malware in collaboration with another individual whom he had met online. He doesn't know anything about his real identity, not even the country in which he lives. The programmer says he never meant to use the application. Instead, he just intended to sell it and let others decide what they wanted to do with it. He also clarified that he took readily available software and only wrote an addition to it. Once the work was done, he gave it to his partner. Experts say the malware has been sold to various cybercriminal groups from Eastern Europe and other parts of the world. One of the operations in which the threat has been used is the one aimed at Target. It's possible that BlackPOS has also been utilized to steal the payment card details of Neiman Marcus customers. In the Target breach, 40 million payment cards have been compromised. The data is being sold on underground markets and is already being misused for fraudulent purchases. To read more click **HERE**

iOS Is the Safest Place to Be, with Mobile Malware Targeting Android 99% of the Time
SoftPedia, 22 Jan 2014: Apple Marketing Chief Phil Schiller has tweeted a link to Cisco's 2014 Annual Security Report, which casts a favorable light on the company's iOS mobile operating system. The report, as its name implies, talks about malware and the frequency of malware encountered by users in all camps, including Apple, Google, Microsoft, and BlackBerry. With an eye on malware that can be installed on the handset itself and wreak havoc as well as online scams and such, Cisco's 2014 Annual Security Report states that 99 percent of all mobile malware is targeted at Android devices, which leaves iOS almost untouched. This being one of the main advantages of using Apple's closed ecosystem, as opposed to the more open Android platform. However, Cisco is careful to point out that these numbers don't necessarily make iOS malware-free. Far from it, actually, as not all types of malware come in the form of an installable package, and not all cyberscams are platform-specific. "Not all mobile malware is designed to target specific devices, however. Many encounters involve phishing, likejacking, or other social engineering ruses, or forcible redirects to websites other than expected," reads the report. "An analysis of user agents by Cisco TRAC/SIO reveals that Android users, at 71 percent, have the highest encounter rates with all forms of web-delivered malware, followed by Apple iPhone users with 14 percent of all web malware encounters." That 14 percent (while not a negligible number) certainly makes iOS seem a lot more secure than Android. Cisco also notes in the report that "Cybercriminals are learning that harnessing the power of the Internet's infrastructure yields far more benefits than simply gaining access to individual computers." "The newest twist in malicious exploits is to gain access to web hosting servers, nameservers, and data centers—with the goal of taking advantage of the tremendous processing power and bandwidth they provide," the Internet company adds. "Through this approach, exploits can reach many more unsuspecting computer users and have

a far greater impact on the organizations targeted, whether the goal is to make a political statement, undermine an adversary, or generate revenue," says Cisco. To read more click **HERE**

Perl Blog Hacked by Islamic Group

SoftPedia, 22 Jan 2014: Hackers of the group called Islamic Cyber Resistance claim to have breached the official blog for the Perl programming language. The hackers say they've targeted the blog in support of the Syrian people and the Syrian Electronic Army. They have not only defaced the blog, but they've also leaked the credentials of close to 3,000 users. The information includes usernames, email addresses, account passwords, and other data. I haven't been able to find the leaked data anywhere else on the web, which indicates that it might be legitimate. At the time of writing, the Perl blog appears to be working properly. A mirror of the defacement is available on zone-h.org. It's worth noting that ICR is somewhat of a controversial group. The hackers have allegedly breached numerous high-profile organizations over the past period. However, an Israeli security expert says the group's hacks are fake, and that they're actually conducting psychological warfare on behalf of Iran. To read more click **HERE**

Orlando Couple Arrested for Role in Massive Phishing Scheme with Nigerian Ties

SoftPedia, 22 Jan 2014: 46-year-old Stephen Barone and his wife, Robin Barone, 44, were arrested last week on suspicion of being involved in a massive phishing scam. The two are said to have stolen around $550,000 (€406,000) from close to 400 people. Authorities say the Orlando couple led a criminal organization that stole the personal details of Wells Fargo and JPMorgan Chase customers with the aid of fake emails. They had used the stolen information to order replacement payment cards, which they had delivered to their own addresses. The fraudulent cards were used to purchase money orders which were deposited into Steve Barone's business account. "The crime was wide reaching, damaging not only the obvious victims, but also other consumers and our business community," said Florida Department of Law Enforcement Commissioner Gerald Bailey. Another FDLE representative has told the Orlando Sentinel that the couple are "tied in with the Nigerians." To read more click **HERE**