Counterintelligence Working Group
NMCIWG Purple Arrow

THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

16 June 2014

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

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, and Sandia National 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 this open source data

June 13, The Register – (International) **Hacker claims PayPal loophole generates FREE MONEY.** A man turned white hat reported a loophole in PayPal's system that can be exploited to earn free money by funneling cash into a mule account before filing for a transaction refund. The company stated that the vulnerability is an issue with its protection policy and did not give additional information about its ability to prevent one-off instances of the scam. Source: http://www.theregister.co.uk/2014/06/13/hacker_claims_paypal_loophole_generates_free_money/

June 12, KPIX 5 San Francisco – (California) **Records of more than 33,000 patients stolen from Santa Rosa radiology facility.** Officials at St. Joseph Health of Sonoma County in Santa Rosa reported June 12 that a thumb drive containing X-ray records of 33,702 patients was stolen during a burglary at an outpatient radiology facility June 2. Patients' personal information was saved on the thumb drive which was taken from a staff member's storage locker. Source: http://sanfrancisco.cbslocal.com/2014/06/12/records-of-more-than-33000-patients-stolen-from-santa-rosa-radioligy-facility/

June 13, The Register – (International) **Entirely new trojan quietly wheeled into black hat forums.** A researcher from RSA reportedly discovered a new trojan, Pandemiya, which contains about 25,000 lines of fresh code and has the ability to steal data from forms, take screen shots to send back to the botmasters who deploy it, and create fake web pages. Pandemiya can be removed by tweaking registry and command line action. Source: http://www.theregister.co.uk/2014/06/13/pricey_ground_up_built_malware_constantly_infects_everything/

June 13, Vallejo Times Herald – (California; Utah) **Utah woman indicted in embezzlement of $1.34 million from Mountain View software firm.** A federal grand jury indicted a former Symantec Corp. employee June 11 on 26 charges of wire fraud and 10 counts of money laundering for allegedly embezzling $1.34 million in funds from the California-based company while working at its Lindon, Utah office between January 2010 and May 2012. The former employee allegedly charged unauthorized personal expenses to company payment cards and made unapproved financial transfers to a shell company used to reallocate funds into her personal bank account. Source: http://www.timesheraldonline.com/news/ci_25956029/san-jose-utah-woman-indicted-embezzlement-1-34

June 12, Securityweek – (International) **Cisco fixes XSS vulnerability in AsyncOS management interface.** Cisco advised customers to update their AsyncOS installations in order to address a cross-site scripting (XSS) vulnerability impacting the Web management interface of the operating system. The flaw affects Cisco Email Security Appliance (ESA) 8.0 and earlier, Cisco Web Security Appliance (WSA) 8.0 and earlier, as well as Content Security Management Appliance (SMA) 8.3 and earlier. Source: http://www.securityweek.com/cisco-fixes-xss-vulnerability-asyncos-management-interface

June 12, Securityweek – (International) **Cybercriminals targeting cloud-based PoS systems via browser attacks.** IntelCrawler researchers dubbed a form of malware, POSCLOUD, which targets vulnerabilities in major Web browsers to compromise cloud-based PoS software typically used by grocery stores, retailers, and other small businesses. The malware relies on keylogging and screenshots to steal personal information and financial data. Source: http://www.securityweek.com/attackers-targeting-cloud-based-pos-systems-browser-attacks

Bell Canada Hacker Arrested and Charged

SoftPedia, 14 Jun 2014: An underage offender was arrested on Friday in Quebec, Canada, in relation to a hacking incident that occurred in February, 2014, directed at a third-party IT supplier of Bell telecommunications company. According to the police, the arrested teen is believed to be part of a hacktivist group called NullCrew, that broke into systems belonging to various businesses as well as schools and government agencies. At the time, NullCrew posted on Twitter that they had managed to hack Bell and provided a link to the leaked information. In an interview, a representative of the group said that Bell had been informed of the vulnerability they had exploited and the fact that customer information could be accessed without authorization. On February 2, a press release from Bell Canada announced that a total of 22,421 user names and passwords belonging to Bell small-business customers had been posted on the Internet the previous weekend. Also leaked were five valid credit card numbers. The hacktivist was charged with one count of unauthorized use of a computer (breaching protected systems) and two counts of mischief in relation to data (spilling the information online) and is scheduled to appear in court on August 19. To read more click HERE

Over 650,000 Domino's Pizza Customer Records Hacked

SoftPedia, 16 Jun 2014: A group of hackers took it to Twitter to announce that they managed to breach the systems of Domino's Pizza in Belgium and France and obtained access to more than 592,000 records belonging to French customers and over 58,000 records belonging to Belgians. The group responsible for the breach is called Rex Mundi, and it appears that the purpose of the deed was money extortion, as a $40,619 demand was forwarded to Domino's Pizza in France for the information not to be made public. The tweet announcing the incident pointed to a file stored on dpaste.de, which has since been removed, informing that the content of the stolen information comprised full names, delivery addresses, phone numbers, email addresses and passwords (hopefully salted and hashed). Domino's Pizza has already reacted to the breach and informed that no credit card data has been stolen, but provided all the other details, and an attacker would have sufficient ammo to initiate phishing campaigns targeting the victims in order to obtain financial details. To read more click HERE

RedHack Hijacks Email Account of Chief of Military Industry Company

SoftPedia, 16 Jun 2014: Members of famous hacktivist group RedHack have announced their latest success – the hijacking of the email account of Izzet Artunç, the head of Mechanical and Chemical Industry Company. Sources inside the group have told Softpedia that the action was a sign or protest against the AKP (the Justice and Development Party) which is the current ruling party within Turkey. The hacktivists have a beef with the party, and ultimately, with Izzet Artunç, as they accuse the government of coordinating work with the Islamic State of Iraq and Syria (ISIS) including through selling weapons, letting others transport it, and transforming Turkey into a "gate to Syria" for radical Islamists. The country's troubles with ISIS have been going on for a while. Back in March, an audio tape landed on YouTube, revealing a conversation between high level Turkish officials, who were discussing a way to justify a military strike in Syria. This particular recording has actually been at the heart of the Turkish YouTube ban, as well as a blockade against social media outlets. Redhack has leaked a trove of conversations belonging to Artunç, whose account they claim has been quite easy to hack into. That's mostly because the security question he set for the email was "What is your name," an incredibly silly slip which further points out just why it is important to have good passwords to protect your online life. To read more click HERE

First Smartphone Malware Drained Battery in Three Hours

SoftPedia, 16 Jun 2014: The numbers regarding mobile malware evolution for 2013 are quite alarming if you consider that, at the beginning of the year, the number of installation packages detected was 6 million and in December the figure grew to almost 10 million. The information was provided by Kaspersky some time ago and showed that Android was the preferred target, 98.05% of the attacks being devised for this platform. Kaspersky also happens to be the security company that performed an analysis of the first smartphone malware ten years ago, back in 2004. As smartphones were relatively new at that moment, the capabilities of the threat were not fully developed, and at the beginning, the malicious file's damage consisted in discharging the battery of the mobile device in about a couple of hours. Eugene Kaspersky described in a blog post the entire process of deciphering the malware, from security researchers getting their hands on the sample to creating a special environment for testing it. The sample, designed for Nokia smartphones (running Symbian), would disseminate through an insecure Bluetooth connection to other devices and would keep looking for new targets to infect. Constant searching for fresh targets would lead to draining the battery of the host "in just two to three hours." The worm, named Cabir by the research team and Caribe by its author, did not have any other functionality and only later malware developments were equipped with money-making capabilities, such as sending messages to premium-rate numbers owned by the cybercriminals themselves. As Eugene Kaspersky puts it, Cabir was created by "the most legendary group of virus writers in history," (29A) and "each creation of 29A was a breakthrough, used afterwards by other virus writers, and then by cybercriminals." 29A was not a group of cybercriminals but of "virus writers creating malware to test and demonstrate new virus technologies." This initial behavior of the malware, which may seem more of a prank to most victims, is equivalent to testing the ability of the threat to spread before it is given functions that deal financial blows to the victim. Since Cabir spread automatically through an insecure connection, it needed a special environment for testing purposes. As such, Kaspersky built a room with zero mobile coverage and with all communications jammed so that viruses could not spread beyond its walls. A highly publicized incident about Cabir occurred in 2005 in Finland, home country of Nokia, during a sports competition. The stadium the event took place at was packed with spectators, one of them owning an infected phone. It so happened that a F-Secure researcher attended the event and got his phone infected. As a result, the security company offered to install a Bluetooth scanner that checked the phones for the Cabir infection. Although Cabir was nothing but a way to test new virus technologies, it later opened the door for cybercriminal activity. Today, sophisticated malware pieces have begun to target mobile users, the latest detection showing that they gained encryption functions used for ransom demands from the victims. To read more click HERE

Microsoft Releases Botched Update on Patch Tuesday, Breaks Down Office 2013

SoftPedia, 16 Jun 2014: After several botched Patch Tuesday rollouts in late 2013, Microsoft has managed to deliver flawless updates to users, with the majority of its customers installing the released fixes without experiencing any issues. Leaving Windows 8.1 Update aside, which itself created some problems for Windows 8.1 users who attempted to install it, most of the patches that came out lately worked pretty well. With the exception of an Office fix rolled out this month, that is. One of the fixes shipped by Microsoft on Patch Tuesday reportedly broke down Office 2013, with many users confirming in a threat on the company's Community forums that the productivity suite no longer works after deploying these updates. Microsoft has already confirmed in a post on the TechNet blogs that it's aware of an issue affecting Office 2013, but said that only 1 percent of its users are actually affected. Surprisingly, there are more than 200 users who have already confirmed on the forums that Office 2013 has been impacted by this bug. Here's what Microsoft said in the post today: ""Shortly after the release of the June Public Update, we received notification of a potential issue affecting a subset of Office 2013 Click-to-Run users. In some cases, users running Office 2013 may not be able to launch Office products after the June Public updates are installed. The Office team is aware of this issue and is working on a solution. Although we have seen this impact less than 1% of our user base, we consider this a high priority issue." Basically, the error that users are getting on their computers is the following: "Something went wrong. We're sorry, but we are unable to start your program. Please ensure it is not disabled by the system. Go online for additional help. Error Code: 30145-4." A Microsoft employee said in a post on the forums that reinstalling Office 2013 is basically the only way to fix this issue and recommends everyone experiencing the aforementioned problem to do the same thing. There are no details right now if Microsoft is preparing another updated or not, so those whose installations have been affected by the problem should proceed with Office 2013 reinstallation as soon as possible. "Shortly after the release of the June 2014 Public Update, we received notification of a potential issue affecting a subset of Office 2013 users. In some cases, users running Office 2013 may not be able to launch Office products after the June Public updates are installed. In order to fix it, first uninstall Office using the fix it, then reinstall Office from the My Accounts page. Note, be sure to have your Microsoft Account and password you used to redeem and install Office," the Microsoft employee said. To read more click HERE

Woman to be first charged under Philippine cybercrime law

AFP, 15 Jan 2014: A woman has been indicted for computer fraud in the first such case under the Philippines' controversial cybercrime law, justice department records showed Sunday. Karla Martinez Ignacio could face up to six years in jail if found guilty of transferring thousands of dollars to her bank account using fraudulent computer data. She was indicted by a prosecutor in the city of Las Pinas, outside Manila, and is set to be charged under the Philippines' Cybercrime Prevention Act. The law is designed to stamp out online scourges like fraud, identity theft and child pornography, but critics say it could be used to stifle dissent as it imposes heavy prison terms for online libel. Facebook and Twitter have become popular ways of organizing major political street protests in the Philippines. The law was passed in 2012 but its implementation was suspended after coming under challenge from various groups. To read more click HERE