The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

11 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

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

February 10, Help Net Security – (International) **Trojan steals Bitcoins and targets OS X.** Researchers at SecureMac identified a new trojan dubbed OSX/CoinThief.A which infects systems running OS X and monitors Internet traffic in order to steal login credentials for Bitcoin wallets and exchanges. The trojan is disguised as an app called StealthBit used to send and receive Bitcoin payments. Source: http://www.net-security.org/malware_news.php?id=2702

February 7, Softpedia – (National) **Bank of America customers targeted in massive Bredo malware distribution campaign.** Researchers at AppRiver identified a large spam campaign capable of avoiding filtering engines that is currently targeting Bank of America customers. Spam email messages carry a variant of the Bredo information-stealing malware that was identified by only 11 antivirus engines. Source: http://news.softpedia.com/news/Bank-of-America-Customers-Targeted-in-Massive-Bredo-Malware-Distribution-Campaign-425067.shtml

February 10, Chicago Sun-Times – (Illinois) **Threatening email closes all DeVry University campuses.** Officials closed all Chicago-area DeVry University campuses February 10 after the university and the Chamberlain College of Nursing received a threatening email February 9. Source: http://www.suntimes.com/news/25499065-418/security-issue-closes-all-devry-university-campuses.html

February 10, Softpedia – (International) **CSRF vulnerability in Instagram allowed hackers to make private profiles public.** A researcher identified and reported a cross-site reference forgery (CSRF) vulnerability in Instagram that could have been used to make private profiles public. Facebook issued a patch in September 2013, and a second patch February 4 to fully address the issue. Source: http://news.softpedia.com/news/CSRF-Vulnerability-in-Instagram-Allowed-Hackers-to-Make-Private-Profiles-Public-425650.shtml

February 10, The Register – (International) **Snapchat bug lets hackers aim DENIAL of SERVICE attacks at YOUR MOBE.** A Telefonica security consultant identified a bug in Snapchat that allows authentication tokens to be reused, which could be exploited to spam users and cause a phone running iOS to freeze or make the app lock up on Android phones. Source: http://www.theregister.co.uk/2014/02/10/snapchat_token_bug_creates_dos_attack_for_ios_android/

February 9, The Register – (International) **RoR Paperclip infested by content type spoofing bug.** A Ruby on Rails developer identified a cross-site scripting (XSS) flaw in the Ruby on Rails Paperclip uploader that could be extended to allow remote code execution. A new version of Paperclip was released that addresses the vulnerability and users were advised to update to it. Source: http://www.theregister.co.uk/2014/02/09/content_type_spoofing_bug_in_ror_paperclip/

February 8, Softpedia – (International) **Expert hacks private repositories on GitHub by combining 5 low-severity bugs.** A researcher found and reported a way to gain access to private GitHub code repositories by combining five low-severity flaws to create a high-severity exploit. GitHub fixed the vulnerabilities and paid a $4,000 reward as part of its bug bounty program. Source: http://news.softpedia.com/news/Expert-Hacks-Private-Repositories-on-GitHub-by-Combining-5-Low-Severity-Bugs-425190.shtml

Hacker Hijacked Supercell Facebook Pages after Breaching Employee's Email Account

SoftPedia, 11 Feb 2014: On Monday, we learned that a Syrian hacker going by the online name of Ethical Spectrum hijacked the Facebook pages for Hay Day and Clash of Clans. It appears that he pulled off the attack after hacking the email account of an employee of Supercell, the Finland-based company that develops the games. The hacker gained access to the Facebook accounts through social media management tool Ergagor. The CEO of Ergagor, Folke Lemaitre, has told Re/code that the hacker gained access to a Supercell employee's email account. He later used this access to breach "several private sources of information," including the Ergagor app used by Supercell to manage the Facebook pages. "Supercell acted quickly on this breach of security and informed Engagor. Engagor responded within minutes by closing down access to the account. At no time Engagor's security as such was breached," Lemaitre said. The hacker has also published a screenshot that shows he had access to information on audience and revenue. However, the Syrian hacker says he hasn't obtained any credit card information from Supercell. As mentioned on Monday, Ethical Spectrum said he simply wanted to help the game development company secure its systems. Since his email, which he had sent to the company's CEO, was ignored, he decided to exploit the security holes he identified. Ever since news broke that Supercell was hacked, many gamers have been sending emails to the hacker asking him for virtual currency. In addition to Supercell, Ethical Spectrum has also targeted an Indonesian hosting company called IDHostinger. However, the organization's representatives are either unaware of the breach, or they're locked out of their Twitter account, since it still contains the posts published by the hacker on Monday. To read more click **HERE**

New POS Malware JackPOS Targets Companies in Canada, Brazil, India and Spain

SoftPedia, 11 Feb 2014: Cybercriminals continue to rely on point-of-sale (POS) malware in order to steal payment card information from companies. Researchers have uncovered a new piece of POS malware which they've dubbed JackPOS. According to IntelCrawler, several attacks using JackPOS have been spotted over the past three weeks. The list of targeted countries includes Brazil, Canada, France, India, Spain, and the United States. Experts have also seen stolen card data from Argentina, Korea and other countries. JackPOS is distributed by cybercriminals through drive-by attacks. The malware is disguised as the Java Update Scheduler. "Several of the found loaders used in detected 'Drive-by' download attack are written using obfuscated compiled AutoIt script, which became quite popular method to avoid AV detection in order to unpack additional binary malicious code and execute further instructions received from the C&C server," IntelCrawler noted in its report. "The bad actors have used some sophisticated scanning, loading, and propagating techniques to attack these vectors to look to get into the merchants system thru external perimeters and then move to card processing areas, which were possibly not separated in compliance with PCI polices." The company's representatives have told Canadian publication The Globe and Mail that JackPOS has been used to compromise close to 700 credit cards in Canada. The details of 3,000 cards have been stolen in Sao Paolo, Brazil. In Bangalore, India, and Madrid, Spain, the number of affected cards is 420 and 230, respectively. It's worth noting that JackPOS is not an entirely new piece of malware. Experts say it's based on code from Alina, another notorious threat designed to steal information from POS terminals. IntelCrawler has published a POS malware infection map that monitors threats such as Alina, BlackPOS (the Trojan used in the Target attack), Dexter and JackPOS. To read more click **HERE**

25 Nigerian Government Websites Hacked by Syrian Anonymous

Softpedia, 11 Feb 2014: Hackers of a group called Syrian Anonymous have managed to deface a total of 25 Nigerian government websites. The list of hacked websites includes the ones of the Ministry of Justice, the Ministry of Finance, the Ministry of Education, the Ministry of Power, the Nigeria Christian Pilgrim Commission, the Federal Neuro Psychiatric Hospital Yaba, the Federal Ministry of Science and Technology and many others. It's uncertain why Syrian Anonymous has targeted these websites. As far as I know, there's no direct conflict between Syria and Nigeria. However, since the hackers are part of the Anonymous movement, it's possible that they've targeted the Nigerian government for other reasons, not necessarily for something that has to do with Syria. At the time of writing, many of the sites are still defaced. Some of them have been restored, while others have been shut down altogether. The complete list of websites and defacement mirrors are available on Pastebin. To read more click **HERE**

Anonymous Hackers Leak Emails from Ukraine's UDAR Party

SoftPedia, 14 Feb 2014: Hackers of Anonymous Ukraine have leaked 130 Mb of emails allegedly stolen from the regional offices of the Ukrainian Democratic Alliance for Reform (UDAR), the party led by politician and former professional boxer Vitali Klitschko. The attack is part of the campaign called OpIndependence, which aims at keeping Ukraine independent from NATO, the EU and other entities. The most interesting of the leaked emails, totaling 9 Mb, have been uploaded separately on several file sharing websites. The hackers accuse the UDAR of "trying to hurl Ukraine into chaos." "We strongly recommend everyone to look through these documents. You will find out a lot of interesting details about how Klitschko and his party dirt not only on their opponents but on their allies too in their race for power and money," the hackers said. They added, "Once again we appeal to the President Yanukovych. People of Ukraine urge you to restore order and bring calm and stability. It's time to disperse this gang of robbers and Nazis! Ukraine must be unified and independent!!" Meanwhile, anti-government protests continue in Ukraine. On Sunday, Al Jazeera reported that 70,000 people gathered on the streets of Kiev demanding a pro-Western government. To read more click **HERE**

Scam Website Targets Army Info

GovInfoSecurity, 10 Feb 2014: The U.S. Army Criminal Investigation Command is warning service members to avoid a false benefits website that's attempting to collect account log-in information for soldiers and veterans. The website, us.militarybenifit.org, is being used to collect U.S. Army service members' Army Knowledge Online e-mail accounts and passwords, according to the Criminal Investigation Command. Army Knowledge Online is the main intranet portal for the military. The bogus website makes the false claim: "The U.S. military has granted access to unclaimed and accumulated Army benefits for the under listed active duty soldiers. Benefits not claimed within the stipulated period will be available for claims after 60 months." Service members are reminded to visit the authorized Army benefits website, myarmybenefits.us.army.mil. "Cyber-crime and Internet fraud presents unique challenges to U.S. law enforcement agencies as criminals have the ability to mask their true identities, locations and cover their tracks quickly," the Army says. "Website and accounts can easily be established and deleted in very little time, allowing scam artists to strike, and then disappear before law enforcement can respond." In other military-related benefits breach news, the U.S. departments of Veterans Affairs and Defense recently experienced a breach of their eBenefits web portal. A software defect exposed information on almost 5,400 of the site's users (see: VA, DoD Breach Exposes Personal Info). The incident occurred during a limited period of time in mid-January during a software upgrade, a spokesperson for the VA said. To read more click **HERE**