The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
20 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 18, Softpedia – (National) **Bank of the West job applicants told that hackers might have stolen their details.** Bank of the West began notifying employment applicants in February that its Web site was breached and any personal information submitted may have been stolen by hackers. Source: http://news.softpedia.com/news/Bank-of-the-West-Job-Applicants-Told-That-Hackers-Might-Have-Stolen-Their-Details-427708.shtml

February 18, SC Magazine – (International) **New variant of Zeus banking trojan concealed in JPG images.** Researchers identified a new variant of the Zeus banking trojan, ZeusVM, that is concealed in a JPG image file to avoid detection by security software. The JPG image files contain the malware configuration files that are needed to launch man-in-the-middle and man-in-the-browser attacks and allow attackers to collect personal information and perform online transactions. Source: http://www.scmagazine.com/new-variant-of-zeus-banking-trojan-concealed-in-jpg-images/article/334477/

February 18, Wall Street Journal – (National) **Nursing homes are exposed to hacker attacks.** Two cybersecurity firms found a Web site containing documents that could allow hackers to potentially obtain electronic medical records and payment information from health care providers. Researchers believe the information was posted by individuals who gained access to SigmaCare software, designed by eHealth Solutions Inc., although the company is unaware of how the files were accessed. Source: http://online.wsj.com/news/articles/SB10001424052702304899704579389171658671940

February 19, Softpedia – (National) **US Army Knowledge Online site inaccessible, hackers take credit for the downtime.** The hacker group DerpTrolling took credit for taking down the U.S. Army Knowledge Online Web site, making it inaccessible for several hours February 19. Source: http://news.softpedia.com/news/US-Army-Knowledge-Online-Site-Inaccessible-Hackers-Take-Credit-for-the-Downtime-427831.shtml

February 19, V3.co.uk – (International) **Microsoft crash reports reveal Houdini hack campaign hitting firms.** A security researcher from Websense found a new hack campaign utilizing the Houdini remote access trojan (RAT) targeting a mobile network operator and government body while cross-referencing Microsoft application and software crash reports. Source: http://www.v3.co.uk/v3-uk/news/2329562/microsoft-crash-reports-reveal-houdini-hack-campaign-hitting-firms

February 19, Network World – (International) **Zeus malware-botnet variant spotted 'crawling' Salesforce.com.** Adallom researchers found that the Zeus trojan, malware known to steal banking credentials, was targeting Windows-based computers in order to swipe business data from the SalesForce Web site through a kind of Web-crawling action. Source: http://www.networkworld.com/news/2014/021914-zeus-malware-278711.html

February 19, Softpedia – (International) **Two different cybercriminal groups are using IE 10 zero-day in their operations.** Security experts believe that two different cybercriminal groups are responsible for an attack on the U.S. Veterans of Foreign Wars Web site and an attack involving the French aerospace industries association, but both groups utilized the same IE zero-day exploit. Source: http://news.softpedia.com/news/Two-Different-Cybercriminal-Groups-Are-Using-IE-10-Zero-Day-in-Their-Operations-427949.shtml

February 19, Softpedia – (International) **DoS, XSS, and data injection flaws fixed in Rails 4.0.3, 3.2.17 and 4.1.0.beta2.** Ruby on Rails released fixes to address three vulnerabilities, including a data injection flaw impacting Active Record, a cross-site scripting (XSS) vulnerability, and a denial-of-service (DoS) issue in Action View. Source: http://news.softpedia.com/news/DOS-XSS-and-Data-Injection-Flaws-Fixed-in-Rails-4-0-3-3-2-17-and-4-1-0-beta2-428015.shtml

February 19, Help Net Security – (International) **US businesses suffered 660,000 internal security breaches.** Researchers at IS Decisions found that in the last 12 months, over 660,000 internal security breaches took place in U.S. businesses, and only about 17 percent of information technology managers consider insider threats to be a top priority for their organization. Source: http://www.net-security.org/secworld.php?id=16379

February 18, Softpedia – (International) **Hackers posted details of 300,000 accounts on Pastebin in the last 12 months.** Researchers discovered that in the last 12 months, over 300,000 accounts' credentials were published on Pastebin through two main sources of information leaks including, insecure Web applications and compromised user machines with installed trojans. Source: http://news.softpedia.com/news/Hackers-Posted-Details-of-300-000-Accounts-on-Pastebin-in-the-Last-12-Months-427658.shtml

US businesses suffered 666,000 internal security breaches

Softpedia, 19 February 2014: Over 666,000 internal security breaches took place in US businesses in the last 12 months, an average of 2,560 per working day, new research has revealed. The findings, revealed by IS Decisions, also found that despite this regular occurrence, only 17.5% of IT managers consider insider threats to be in their top three security priorities. The new report [**LINK**] highlights the issue of internal security as a greater challenge for larger organizations, with 40% of businesses of over 500 employees having had internal security breaches in the last year. It also compares the occurrence of and IT professional's attitudes towards insider threats in the UK, where the trend was echoed with just 21% voicing concern despite over 300,000 internal security breaches in the last year. Insider threats continue to be a relatively low priority for IT professionals, with the research finding the issue is trumped by concern about the threats of viruses (67%), data loss (47%) and hacking (39%). Yet the numbers suggest that the greatest source of data loss is in fact from employees, indicating that IT professionals are negating to look at their own internal structures seriously enough to address their own concerns. Francois Amigorena, CEO of IS Decisions commented, "It is human nature to see external sources as your greatest threat, and that coupled with the fact that insider threat is a complex issue to manage has led to IT professionals seemingly turning a blind eye to the issue. "These numbers, and the impact that the Edward Snowden case had last year, show clearly that internal security should be higher up the IT agenda. The reality is that it is a very considerable problem, but the good news is that there is a lot that IT departments can do to mitigate the risks. It's a technology issue as well as a cultural one, and can be addressed from both of these angles." To read more click **HERE**

More Damage Uncovered in Las Vegas Sands Hack

FOX News, 19 Feb 2014: A cyber breach of Las Vegas Sands (LVS) that caused a six-day website outage appears to have done far more damage than the casino operator previously realized. Hackers who took credit for the cyber attack posted images online that suggested the intrusion was carried out by politically-motivated hackers, or hacktivists, angered by Las Vegas Sands CEO Sheldon Adelson's close ties to Israel. The images also showed the hack compromised some employee data, including Social Security numbers and email addresses. However, an 11-minute video posted on YouTube also appears to show the attack uncovered the passwords for administrator and slot systems and information from players at the Sands casino in Bethlehem, Pa., according to published reports. The video has since been removed from Google's (GOOG) YouTube. "We have now determined that the hackers reached at least some of the company's internal drives in the U.S. containing some office productivity information made up largely of documents and spreadsheets," a Las Vegas Sands spokesman said in an emailed statement. "We have seen the video and are continuing to investigate what, if any, customer or additional employee data may have been compromised as part of the hacking." In response to the hack, Sands Bethlehem offered all employees free credit monitoring and identity theft protection services. The intrusion was first revealed last week, preventing guests from using the websites of certain casinos, including the Venetian and Palazzo casinos in Las Vegas and the company's casinos in Singapore and Macau. Online access was not restored until Monday and the company's e-mail system was restored last Friday. Sands said it continues to believe that the company's "core operating systems have not been impacted." It's not clear who carried out the cyber attack on Sands, but law enforcement agencies are investigating. The casino operator said it continues to work with state and federal officials as well as outside experts to "determine the identity of the hackers and the overall extent of the hacking." Images posted online last week included comments critical of Adelson, the casino giant's billionaire CEO. "Encouraging the use of Weapons of Mass Destruction, UNDER ANY CONDITION, is a Crime," one message read, signed by the "Anti WMD Team." The message also included a picture of Adelson hugging Israeli Prime Minister Benjamin Netanyahu. The comments appeared to be in response to remarks made by Adelson last year suggesting a nuclear bomb should be dropped on the Iranian desert in order to facilitate negotiations over the country's nuclear program. Shares of Sands fell 0.36% to $80.45 Wednesday afternoon, trimming their 12-month gain to 57%. To read more click **HERE**