The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

23 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

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

January 21, Krebs on Security – (National) **DHS alerts contractors to bank data theft.** A U.S. Department of Homeland Security (DHS) spokesman stated that documents belonging to 114 contractor organizations that bid on a DHS Science & Technology division contract could have been disclosed by a security breach that occurred in late 2013, with 16 documents containing banking information. Source: http://krebsonsecurity.com/2014/01/dhs-alerts-contractors-to-bank-data-theft/

January 22, Washington Post – (National) **VA software glitch exposed veterans' personal information.** The U.S. Department of Veterans Affairs (VA) announced January 21 that it conducted a full review of a software glitch and remedied a defect in their online benefits portal, after an issue on a joint VA and U.S. Department of Defense site January 15 potentially exposed private information of more than 5,300 military veterans and their dependents to anyone that accessed the site. The site was brought back online January 19 and officials continue to investigate the incident. Source: http://www.washingtonpost.com/blogs/federal-eye/wp/2014/01/22/va-software-glitch-exposed-veterans-personal-information/

January 22, Softpedia – (International) **Russia accused of conducting global cyber espionage campaign.** Researchers at CrowdStrike identified a large cyber espionage campaign targeting energy, government, defense, and other organizations in the U.S., Europe, and Asia operated by a group dubbed Energetic Bear that appears to be affiliated with the Russian government. The campaign has been monitored since August 2012 and relies on the HAVEX RAT and SYSMain RAT remote access trojans (RATs.) Source: http://news.softpedia.com/news/Russia-Accused-of-Conducting-Global-Cyber-Espionage-Campaign-419457.shtml

January 22, Threatpost – (International) **XSS filter bypass bug found in Chrome and Safari.** A researcher at Eleven Paths warned of a flaw in anti-cross site scripting (XSS) filters in the Chrome and Safari browsers that could be exploited to allow an attacker to bypass the filters and use XSS flaws on certain Web sites to compromise users' systems. The researcher released a proof-of-concept for the vulnerability. Source: http://threatpost.com/xss-filter-bypass-bug-found-in-chrome-and-safari/103761

January 21, PCWorld – (International) **Syrian Electronic Army hacks Microsoft's Office Blogs site mere hours after redesign.** Attackers claiming affiliation with the Syrian Electronic Army hacktivist group compromised Microsoft's official Office Blogs site January 20. Microsoft reset the site's account and regained control later that day. Source: http://www.pcworld.com/article/2089820/syrian-electronic-army-hacks-microsofts-office-blogs-site.html

Snapchat's Account Registration CAPTCHA System Hacked

SoftPedia, 23 Jan 2014: Snapchat has been having a lot of security-related problems lately. After someone leaked the details of 4.6 million customers, now experts have managed to hack the newly introduced CAPTCHA system. The system is designed to prevent bots from registering accounts. Users are presented with nine images and they have to select those that contain the Snapchat ghost. However, shortly after Snapchat announced the new security feature, a man named Steve Hickson managed to write a piece of code that can automatically solve the puzzle. It took him around 30 minutes to develop a program that has less than 100 lines. "With very little effort, my code was able to 'find the ghost' in the above example with 100% accuracy," Hickson explained. "It's a numbers game with computers and Snapchat's verification system is losing." Hickson is not the only one who cracked the CAPTCHA. 16-year-old Graham Smith, who has identified a number of Snapchat security issues over the past period, says he has also written a script for solving the puzzle. The expert has told TechCrunch that "Snapchat is doomed forever as far as security" if it doesn't take some measures. To read more click **HERE**

Website of Brazil's City of Franca Hacked, Redirects Users to Malicious Site

SoftPedia, 23 Jan 2014: Brazilian government websites are often the target of cyberattacks. Not only do hacktivists that target them, but also cybercriminals. F-Secure researchers have spotted a piece of malicious code in a JavaScript file on the official website of the city of Franca in São Paulo, Brazil (franca.sp.gov.br). The code loads a Flash object (Trojan:SWF/Redirector.EQ) that redirects the site's visitors to a malicious domain. According to experts, the attackers have most likely exploited a vulnerability in the outdated Joomla version running on the website. F-Secure has reached out to Brazil's Computer Security and Incident Response Team to let them know about the attack. A simple search on Twitter shows that at least 5 government sites have been hacked over the last 24 hours. To read more click **HERE**

Armenian Government Websites Hacked and Defaced by Azerbaijani Group

SoftPedia, 23 Jan 2014: Hackers of the Azerbaijani group called Anti-Armenia Team have breached and defaced a total of 64 Armenian websites. Some of them belong to the country's government and other high-profile organizations. According to HackRead, the list of targets includes the Ministry of Education, the police, the Football Federation of Armenia, the Artsakh State University, and the Ministry of Urban Development. At the time of writing, the websites have been restored. Some of these websites were breached and defaced last year by the same group, which indicates that the Armenian government does a poor job securing its sites. The cyberattacks launched by the Anti-Armenia Team are carried out in support of Azerbaijan in the country's territorial dispute with Armenia over the Nagorno-Karabakh state. To read more click **HERE**

Notorious hacker picked up in Romania

NY Post, 23 Jan 2014: A former cabdriver, Marcel Lazarus Lehel — known as Guccifer — was busted in his Romanian village Wednesday with the help of the US Secret Service. Guccifer became infamous on the Web by leaking self-portraits of former President George W. Bush, as well as e-mails between Colin Powell and a 30-years-younger Romanian female diplomat that prompt-ed the former secretary of state to deny he was having an affair. Lehel, 40, was tracked down to the village of Paulis, where he lived with his wife and kindergarten-age daughter and rarely went outside. "I heard he spent all day at the computer," the town's mayor, Peter Nicoara, told the newspaper Adevarul. Two weeks ago, the Web site The Smoking Gun, which posted much of Guccifer's hacked material, said his victims included show-biz figures such as Steve Martin, Rupert Everett and Mariel Hemingway, former Nixon White House figure John Dean, three members of the House of Lords, authors Candace ("Sex and the City") Bushnell and Kitty Kelley, editor Tina Brown and the director of Romania's domestic intelligence service, George-Cristian Maior. To read more click **HERE**