THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

7 August 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

DHS contractor suffers major computer breach, officials say

The Washington Post, 7 Aug 2014: A major U.S. contractor that conducts background checks for the Department of Homeland Security has suffered a computer breach that probably resulted in the theft of employees' personal information, officials said Wednesday. The company, USIS, said in a statement that the intrusion "has all the markings of a state-sponsored attack." The breach, discovered recently, prompted DHS to suspend all work with USIS as the FBI launches an investigation. It is unclear how many employees were affected, but officials said they believe the breach did not affect employees outside the department. Still, the Office of Personnel Management has also suspended work with the company "out of an abundance of caution," a senior administration official said. "Our forensic analysis has concluded that some DHS personnel may have been affected, and DHS has notified its entire workforce" of the breach, department spokesman Peter Boogaard said. "We are committed to ensuring our employees' privacy and are taking steps to protect it." The intrusion is not believed to be related to a March incident in which the OPM's databases were hacked, said officials, some of whom spoke on the condition of anonymity because they were not authorized to speak on the record. That intrusion was traced to China and none of the personal data, which was encrypted, was stolen. In the DHS case, said a second senior administration official, "We have an inclination that, based on what the company has been telling us, there has been a spill. The degree to which that information has been exfiltrated for other purposes is what we're trying to discern now." Officials said that, although the DHS encrypts the employee data it sends USIS, it's unclear whether the data remain encrypted. USIS, a Falls Church, Va., company, is the largest provider of background investigations for the federal government. It conducts checks for DHS employees and applicants who require security clearances. While the OPM manages the bulk of federal background investigations, some departments, such as Homeland Security, have authority to hire contractors for their own investigations, officials said. Company officials said they recently discovered the penetration of the firm's corporate network and informed the FBI, the OPM and other relevant agencies. "We are working collaboratively with OPM and DHS to resolve this matter quickly and look forward to resuming service on all our contracts with them as soon as possible," the firm said in its statement. The U.S. government and its contractors are a favorite target for hackers who are interested in obtaining sensitive data, ranging from employee information contracts to weapons-system designs. The U.S. Computer Emergency Readiness Team (US-CERT), a component of DHS, is conducting an on-site assessment at USIS, including a forensic analysis. Officials said they are seeking to learn exactly what happened and who was behind the intrusion. US-CERT has also instructed the company on how to mitigate the breach, officials said. Some lawmakers have announced they will investigate the breach. "It is extremely concerning that the largest private provider of background investigations to the government was hacked," said Rep. Elijah E. Cummings (Md.), the ranking Democrat on the House Oversight and Government Reform Committee. "I am asking Chairman [Darrell] Issa to work with me in having our committee investigate this matter with the utmost urgency." The USIS breach "is very troubling news," said Sen. Jon Tester (D-Mont.), a Homeland Security Committee member. "Americans' personal information should always be secure, particularly when our national security is involved. An incident like this is simply unacceptable." To read more click **HERE**

August 6, Securityweek – (International) **PayPal confirms new two-factor authentication bypass issue.** Researchers with Escalate Internet identified a way to bypass PayPal's two-factor authentication (2FA) mechanism with companies that use Adaptive Payments, as the method Adaptive Payments uses to connect PayPal accounts to the application only requires a login and password with no 2FA. PayPal stated that they are aware of the issue and working on a fix. Source: http://www.securityweek.com/paypal-confirms-new-two-factor-authentication-bypass-issue

August 5, Utah County Daily Herald – (Utah) **Police: BYU student hacked into school computers to change grades.** A Brigham Young University student was arrested and charged after allegedly confessing to police that he breached the Utah university's cyber security remotely to change his student status, illegally accessed a professor's computer and other staff members' computers to obtain logins and passwords in order to modify grades, and downloaded pages of personal information belonging to students without authorization. Source: http://www.heraldextra.com/news/local/crime-and-courts/police-byu-student-hacked-into-school-computers-to-change-grades/article_1d68bda3-ab1e-5ecb-a7ce-6757c8bda858.html

August 6, Securityweek – (International) **Synology NAS devices hit in ransomware attack, firm advises upgrade.** Synology stated that it confirmed user reports of infections by the SynoLocker ransomware on the company's Diskstation devices and found that Synology network-attached storage (NAS) servers running DSM 4.3-3810 and earlier were compromised by exploiting a vulnerability that was patched in December 2013. Users were advised to upgrade their DSM installations to close the vulnerability. Source: http://www.securityweek.com/synology-nas-devices-hit-ransomware-attack-firm-advises-upgrade

August 6, Softpedia – (International) **Magnitude Exploit Kit is a well-oiled crimeware.** Trustwave researchers analyzed the Magnitude Exploit Kit used to infect several high-profile Web sites and found that the malware relied on one Internet Explorer exploit and two Java exploits, and had a 20 percent infection success rate within 1 month, among other findings. Source: http://news.softpedia.com/news/Magnitude-Exploit-Kit-Is-a-Well-Oiled-Crimeware-453744.shtml

August 5, Securityweek – (International) **Over 90% of enterprises exposed to man-in-the-browser attacks: Cisco.** Cisco released its Midyear Security Report August 5, which found that around 94 percent of its customers have issued domain name system (DNS) requests to hostnames with IP addresses associated with the distribution of malware that contains man-in-the-browser (MitB) capabilities. The report also found that aviation, chemical, pharmaceutical, and media and publishing industries had the highest rates of malware encounters, among other findings. Source: http://www.securityweek.com/over-90-enterprises-exposed-man-browser-attacks-cisco

August 5, Softpedia – (International) **Security flaw in Spotify for Android may enable phishing.** Trend Micro researchers identified a vulnerability in the Spotify app for Android that could allow attackers to take control of what is displayed in the app's interface, which could potentially be used for phishing or redirection to malicious pages. Spotify stated that they released an update that closes the vulnerability after being notified and advised all users to update to the latest version. Source: http://news.softpedia.com/news/Security-Flaw-in-Spotify-for-Android-May-Enable-Phishing-453633.shtml

Symantec issues update fixing Endpoint Protection zero-day
Heise Security, 7 Aug 2014: Symantec has issued updates for its Endpoint Protection solution that fix the zero-day escalation of privilege vulnerability recently discovered by Offensive Security researchers. "The issue, as reported, affects the Application and Device Control component of Symantec Endpoint Protection. This vulnerability is not accessible remotely and only affects SEP clients actually running Application and Device Control," the company explained in the updates advisory. "If the vulnerability is exploited by accessing the computer directly, it could result in a client crash, denial of service, or, if successful, escalate to admin privileges and gain control of the computer," they say, and noted that they are not aware of instances of exploitation of this vulnerability. They also noted that the vulnerability can't be exploited remotely, but as Offensive Security published the exploit code, the danger is very real. The vulnerability affects all versions of Symantec Endpoint Protection clients 11.x and 12.x running Application and Device Control, and users are advised to update to 12.1 RU4 MP1b. Symantec Endpoint Protection 12.0 Small Business Edition is also affected, and users can remove the danger by updating to latest available build of SEP 12.1 Small Business Edition, which is not affected. Symantec is expected to address the other zero-days found in its Endpoint Protection solution in due time. Offensive Security has shared

information about some of the found vulnerabilities with CERTs, but others have been studied during the company's Advanced Windows Exploitation (AWE) course at the Black Hat 2014 conference this week. To read more click **HERE**

PF Chang's data breach lasted 8 months

Heise Security, 5 Aug 2014: Asian-themed US restaurant chain P.F. Chang's China Bistro has finally provided some more details about the breach it suffered earlier this year, including the 33 restaurant locations where the security of their PoS systems was compromised. The company first found out about the compromise on June 10, 2014, when it was alerted by the US Secret Service. On the very next day, they moved to a manual processing system for all credit and debit card transactions. Once the affected hardware has been replaced, they went back to their standard card processing system. The subsequent investigation revealed that the initial intrusion dates back to October 10, 2013. The company believes that the thieves made away with card numbers and, in some cases, also the cardholder's name and/or the card's expiration date. The investigation is still ongoing, and there could be more revelations. "P.F. Chang's is taking steps to protect your credit card information. You are automatically protected with AllClear Secure for the next 12 months – there is no action required on your part to receive this service," they wrote, adding that it would be a good idea for them to contact credit bureaus and ask them to place a fraud alert on their files. The stolen card data has appeared for sale on well-known carder store Rescator(dot)so in June, and was sold for prices between $18 to $140 per card. To read more click **HERE**