THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

22 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

August 20, Computerworld – (National) **UPS now the third company in a week to disclose data breach.** The United Parcel Service (UPS) announced August 20 that a security breach at 51 of its UPS Stores in 24 States may have exposed the personal information, including addresses and payment card information, of customers who completed transactions between January 20 and August 11. An investigation found previously unknown malware was installed on individual stores' systems but did not affect wider UPS networks. Source: http://www.computerworld.com/s/article/9250545/UPS_now_the_third_company_in_a_week_to_disclose_data_breach

August 20, Softpedia – (Michigan) **Traffic lights system hacked in Michigan.** A team of researchers in Michigan conducted an experiment and were able to access nearly 100 wirelessly networked traffic lights and cameras and found that the network can be easily accessed because of a lack of encryption, vulnerability to known exploits, and default logins and passwords. Source: http://news.softpedia.com/news/Traffic-Lights-System-Hacked-in-Michigan-455713.shtml

August 18, Kansas City Star – (Kansas) **Online data breach affects employees of Children's Mercy Hospital.** StayWell Health Management notified 4,076 Children's Mercy Hospital employees and spouses that their personal information was stolen in a breach discovered in an online scheduling application stored by Onsite Health Diagnostics. The third-party vendor removed the data from the affected system, which included names and phone numbers, among other information that was collected in 2012. Source: http://www.kansascity.com/news/business/technology/article1250544.html

August 21, Help Net Security – (International) **Most popular Android apps open users to MITM attacks.** FireEye researchers conducted an analysis of the 1,000 most popular free Android apps in the Google Play store and found that many contain one or more vulnerabilities that could leave users vulnerable to man-in-the-middle (MitM) attacks. Source: http://www.net-security.org/secworld.php?id=17279

August 20, Securityweek – (International) **Graphic library flaw exposes apps created with Delphi, C++ Builder.** Researchers with Core Security reported identifying a security vulnerability that can affect software with a specific version of Embarcadero C++ Builder XE6, Embarcadero Delphi XE6, and possibly other versions. Embarcadero products are used by organizations and companies in industries including healthcare, financial services, and other industries to develop in-house applications. Source: http://www.securityweek.com/graphic-library-flaw-exposes-apps-created-delphi-c-builder

Sneak attack through smartphone shared memory
Heise Security, 22 August 2014: A weakness believed to exist in Android, Windows and iOS operating systems could be used to obtain personal information from unsuspecting users, research at the University of Michigan has shown. The team demonstrated the hack in an Android phone. The method was successful between 82 percent and 92 percent of the time on six of the seven popular apps they tested. Gmail, CHASE Bank and H&R Block were among those easily compromised.

The hack is particularly dangerous because it allows attackers to time the moment that they present the user with a fake screen to when the user is expecting to enter sensitive data. "We know the user is in the banking app, and when he or she is about to log in, we inject an identical login screen," said Qi Alfred Chen, a doctoral student in electrical engineering and computer sciences at U-M. "It's seamless because we have this timing." Chen, who works under Zhouqing Morley Mao, an associate professor electrical engineering and computer sciences at U-M, will present the research on Friday, Aug. 22 at the 23rd USENIX Security Symposium in San Diego, Calif. Chen, Mao, and co-author Zhiyun Qian, an assistant professor at the University of California, Riverside, believe their method will work on other operating systems in which apps can access the phone's shared memory freely. This feature allows processes to share data efficiently, but it also allows malware to track user behavior. Even if that channel was blocked, Chen believes that other connections may be exploited to achieve the same end. "The assumption has always been that these apps can't interfere with each other easily," said Qian, a recent doctoral graduate from Mao's group. "We show that assumption is not correct, and one app can in fact significantly impact another and result in harmful consequences for the user." The attack starts when a user downloads a seemingly benign app, controlling the phone's wallpaper for instance. When that app is running in the background, attackers can access the shared memory without needing any special privileges. The researchers monitored changes in the shared memory and correlated the changes to what they call an "activity transition events." These included logging into a service or photographing a check so that it could be deposited online. Augmented with a few other side channels, the team could fairly accurately track user activity in real time. Chen suggests that check images are a particular risk. "A camera-peeking attack can steal your account number, home address and even your signature," he said. Of the seven apps, Amazon gave the team the most trouble, with a 48 percent attack success rate. This is an accident of the app's flexibility – it allows one activity to transition to almost any other activity, increasing the difficulty of guessing what the user will do next. Asked what a smart phone user can do about this situation, Qian said, "Don't install untrusted apps." To read more click **HERE**