THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

22 October 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

Samsung devices get top US security clearance

AFP, 21 Oct 2014: South Korean tech giant Samsung said Tuesday its smartphones and tablets have received a US government security clearance allowing officials to use them to send classified information. The Samsung devices were placed on a list of gadgets approved by the National Security Agency for managing classified information. The Boeing Black phone is also on the list. The newly approved devices include the Galaxy S4, Galaxy S5, Galaxy Note 3 and Galaxy Note 10.1 tablet. They can all use Samsung's Knox software, which adds a layer of security for data on the devices. Samsung products had already been on the US Defense Department list of approved hardware for "sensitive but unclassified" use, but the latest approval expands that to more secret information. The approval "proves the unmatched security of Samsung Galaxy devices supported by the Knox platform," said JK Shin, who heads the company's IT and mobile business. With the latest approval, Samsung -- the world's largest smartphone maker -- can now seek a wider range of US government contracts for its mobile devices. To read more click **HERE**

Google improves account security with special USB key

Fox News, 22 Oct 2014: With countless security breaches taking place where data such as usernames and passwords falls into the hands of cybercriminals, Internet users are being increasingly encouraged to enable two-step verification with Web services that offer it. This extra layer of security forces you to enter a dynamically generated code sent to a mobile device, together with the usual password. This beats hackers as they'd need not only your password, but your mobile device too, in order to break into your account. While this might sound like enough to protect your Web accounts, Google on Tuesday announced its adding "even stronger protection" for its own online services, a move that it says is aimed at providing peace of mind for "particularly security-sensitive individuals." The method, called Security Key, uses the Universal 2nd Factor (U2F) protocol from the FIDO (Fast Identity Online) Alliance. It involves first pairing a small device, the key, with your Google account. After that, each time you log in with your password, you simply insert the key into your computer's USB port, wait for a prompt (eg. a flashing light on the device), give it a tap, and you're in. A notable advantage of the key is that it offers improved protection against phishing scams as it only works with genuine Google sites rather than imitation sites designed to trick you into handing over sensitive data, such as your password. "When you sign into your Google Account using Chrome and Security Key, you can be sure that the cryptographic signature cannot be phished," Google's Nishit Shah wrote in a blog post announcing the company's new security measure. However, be aware that if you're logging in using a tablet that has no USB port, you'll have to fall back on one of your other two-step verification options. Also, as Shah alludes to above, accessing your Google account using the key can currently only be done via the company's Chrome browser. "It's our hope that other browsers will add FIDO U2F support," Shah said in his post. "As more sites and browsers come onboard, security-sensitive users can carry a single Security Key that works everywhere FIDO U2F is supported." To read more click **HERE**

October 21, IDG News Service – (International) **One week after patch, Flash vulnerability already exploited in large-scale attacks.** Researchers identified an exploit kit sold on underweb forums known as Fiesta that is bundled with an exploit for a recently-patched Flash Player vulnerability. Users were advised to apply the patch that was issued October 14. Source: http://www.networkworld.com/article/2836733/one-week-after-patch-flash-vulnerability-already-exploited-in-largescale-attacks.html

October 21, Securityweek – (International) **Cisco products vulnerable to POODLE attacks.** Cisco is analyzing its products to determine which may be affected by the POODLE vulnerability in Secure Sockets Layer (SSL) and released a list of confirmed vulnerable products, which includes Cisco Webex Social, Cisco ACE, Cisco Wireless LAN Controller, and several other products. Source: http://www.securityweek.com/cisco-products-vulnerable-poodle-attacks

October 21, The Register – (International) **Palo Alto Networks boxes spray firewall creds across the net.** A researcher found that misconfigured Palo Alto Networks firewalls could allow attackers to gain user and domain names and passwords, potentially exposing customer services such as VPNs and webmail. Palo Alto Network advised users to apply best practice guidelines developed by the company. Source: http://www.theregister.co.uk/2014/10/21/palo_alto_customers_spray_net_with_firewall_creds/

October 21, Softpedia – (International) **Staples investigates possible card data breach.** Officials at retail chain Staples are investigating to determine if the payment processing systems of 11 stores in 7 States were compromised after receiving reports from several financial intuitions of fraudulent activity being recorded on payment cards held by Staples customers. Source: http://news.softpedia.com/news/Staples-Investigates-Possible-Card-Data-Breach-462670.shtml

Windows 0-day exploited in ongoing attacks, offers temporary workarounds

Heise Security, 22 Oct 2014: Microsoft is warning users about a new Windows zero-day vulnerability that is being actively exploited in the wild and is primarily a risk to users on servers and workstations that open documents with embedded OLE objects. The vulnerability is currently being exploited via PowerPoint files. These specially crafted files contain a malicious OLE (Object Linking and Embedding) object. "Object Linking & Embedding (OLE) is legitimately used to display parts of a file within another file, e.g. to display a chart from an Excel Spreadsheet within a PowerPoint presentation," noted Mark Sparshott, EMEA director at Proofpoint. "This is not the first time that a vulnerability in OLE has been exploited by cybercriminals, however most previous OLE vulnerabilities have been limited to specific older versions of the Windows operating system. What makes this vulnerability dangerous is that it affects the latest fully patched versions of Windows." "User interaction is required to exploit this vulnerability," Microsoft explained in the security advisory. "In an email attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted file to the user. For this attack scenario to be successful, the user must be convinced to open the specially crafted file containing the malicious OLE object. All Microsoft Office file types as well as many other third-party file types could contain a malicious OLE object." "In a web-based attack scenario, an attacker would have to host a website that contains a specially crafted Microsoft Office file, such as a PowerPoint file, that is used in an attempt to exploit this vulnerability," they noted. "In addition, compromised websites (and websites that accept or host user-provided content) could contain specially crafted content that could exploit this vulnerability. An attacker would have no method to force users to visit a malicious website. Instead, an attacker would have to persuade the targeted user to visit the website, typically by getting them to click a hyperlink that directs a web browser to the attacker-controlled website." A successful exploitation could lead to the attacker gaining same user rights as the current user, and if that means administrative user rights, the attacker can install programs; access, modify, or delete data; or create new accounts with full user rights. The vulnerability affects all supported Windows versions, and there is currently no patch for it. Microsoft is still investigating the matter and deciding whether they will issue an out-of-band patch or wait for the next Patch Tuesday to plug the hole. In the meantime, the company has shared workarounds that help block known attack vectors. Users can implement a specific Fix It solution; enable User Account Control (UAC) as it displays a prompt before a file containing the exploit is executed; and deploy the Enhanced Mitigation Experience Toolkit 5.0 and configure Attack Surface Reduction (instructions can be found **here**). In addition to all this, they would do well not to open Microsoft PowerPoint files, Office files, or any other files received or downloaded from untrusted sources. "Users should also always be mindful of emails containing links or files even from sources they trust. It's better to delete and ask the sender to send again than to chance

being infected and opening up your whole business network to malware attack," Mark James, security expert at ESET, pointed out. "The race is on," warns Sparshott. "Cybercriminals will use phishing and longlining emails containing URL links to websites hosting malicious files that exploit this vulnerability or attach the malicious file to the email itself. While Microsoft and security vendors rush to close the security hole the best form of defense remains using the latest next generation detection technologies such as sandboxing at the email gateway to prevent the emails reaching users in the first place. Organisations not yet using advanced detection tools will need to fall back to notifying users and relying on them not to click the links and open files, unfortunately Proofpoint's Human Factor Report highlighted that staff click on 1 in 10 malicious links on average so cybercriminals will see a lot of success before the security gap on this vulnerability is closed." To read more click **HERE**

Nearly Half of Consumers Will Punish Breached Retailers during Holidays

DarkReading, 21 Oct 2014: Consumers say they'll talk with their wallets if they hear their favorite store has played fast and loose with customer data.The data breach gremlins could be coming home to roost for retailers this holiday season, and they're not coming by way of regulators or investors. According to a survey released this weekend, it's the consumers themselves who are holding retailers accountable. Conducted by Princeton Survey Research Associates on behalf of CreditCards.com, the survey showed that nearly half of consumers today would be less likely to shop at a store during the holiday season if that establishment suffered a breach. The results show that 45% of consumers reported that they "probably" or "definitely" would avoid a store over the holidays if they found out it had a data breach. Further, the news of retail breaches has made consumers somewhat allergic to plastic -- approximately 48% say the bad press has made them more likely to use cash in favor of cards. Beyond surveys like these, it has been difficult to calculate the losses suffered by retailers, such as Target and Home Depot, from changes of consumer and investor habits following big breaches. Last February, Target reported a 46% drop in profit in the financial quarter following the disclosure of its massive breach. However, it is hard to know if that was truly caused by the breach or simply correlated with it. There were other market forces at play then, including a costly expansion into Canada, according to The Wall Street Journal (subscription required). More recently, neither Home Depot nor JPMorgan Chase has experienced stock dips as a result of their megabreaches. Some industry watchers have cited Home Depot's recent 2% stock uptick following the disclosure of its breach as evidence that consumers are experiencing "breach fatigue", and that retailers shouldn't fear long-term breach fallout. But on the flip side of this argument, it could just as easily be evidence of a strengthening overall market. In support of this, just last week the National Retail Federation reported that the average shopper plans to spend 5% more this year during the holiday shopping season than last year's busy season. In spite of the inconclusive market data, consumer surveys have repeatedly shown that consumers are growing fed up with their merchants for shoddy security around sensitive information. In fact, just last month, HyTrust ran a survey that showed results similar to the one out this week. In that survey, 51% of consumers reported that they take business elsewhere after a breach that compromises information like addresses, Social Security numbers, and credit card details. More than a third of consumers said they believe the worst kinds of breaches are those that compromise Social Security numbers. Taking things a step further, the HyTrust poll showed that more 45% of consumers believe that corporate officers should be held accountable for breaches at their organizations, and that the companies should be considered "criminally negligent." And this year, Javelin Research found that 54% of consumers would switch healthcare providers after a breach, 40% would switch banks, and 30% would shop at different retailers. To read more click **HERE**