THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

25 September 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

September 24, Softpedia – (International) **New Tinba banking trojan variant is stealthier, uses public key signing.** Researchers from Trusteer analyzed an updated variant of the Tiny Banker (also known as Tinba) financial malware and discovered that the authors added a domain generation algorithm (DGA) and fitted it with user-mode rootkit capabilities and a verification process to make sure that messages are sent from an authentic bot master. Source: http://news.softpedia.com/news/New-Tinba-Banking-Trojan-Variant-Is-Stealthier-Uses-Public-Key-Signing-459834.shtml

September 23, WFIE 14 Evansville – (Kentucky) **Data breach at Owensboro medical practice.** Owensboro Medical Practice and its business associate Research Integrity in Kentucky notified about 3,000 patients of a data breach after the medical practice learned that former employees allegedly stole the information in 2011 in an attempt to contact patients to join them in their own business. Source: http://www.14news.com/story/26609328/data-breach-at-owensboro-medical-practice

September 24, Threatpost – (International) **Mozilla to part ways to SHA-1.** Mozilla asked Certificate Authorities and Web sites to upgrade certificates to SHA-256, SHA-384, or SHA-512 after experts reported that SHA-1 will be practical for collision attacks by 2018. Mozilla will release warnings to update certificates on versions of Firefox in early 2015. Source: http://threatpost.com/mozilla-latest-to-part-ways-with-sha-1/108495

September 24, Help Net Security – (International) **Mitigations for Spike DDoS toolkit-powered attacks.** Akamai Technologies released an advisory alerting enterprises of the Spike distributed denial of service (DDoS) toolkit that runs on a Windows system and can launch infrastructure-based and application-based DDoS payloads including SYN flood, UDP flood, GET flood, and Domain Name system (DNS) query floods. The toolkit can be mitigated be implementing access control lists (ACLs). Source: http://www.net-security.org/secworld.php?id=17406

September 23, The Register – (International) **Apple's new iPhone 6 vulnerable to last year's TouchID fingerprint hack.** Lookout researchers found that a vulnerability that could allow access into Apple's iPhone 6 and 6 Plus models through their TouchID fingerprint sensors remained unpatched. Scammers can unlock the devices by creating a fake fingerprint, the same flaw that was found in the iPhone 5S model in 2013. Source: http://www.theregister.co.uk/2014/09/23/iphone_6_still_vulnerable_to_touchid_fingerprint_hack/

Critical SSL flaw patched in Firefox, Thunderbird, Chrome
Heise Security, 25 Sep 2014: If you are a Mozilla Firefox, Thunderbird or Seamonkey user, you should implement the latest patches issued by the company as soon as possible, as they fix a critical bug whose exploitation can lead to successful Man-in-the-Middle attacks. The bug affects all versions of the Mozilla NSS library, and makes it vulnerable to a variant of a signature forgery attack previously published by Daniel Bleichenbacher, Mozilla has explained. "This is due to lenient parsing of ASN.1 values involved in a signature and could lead to the forging of RSA certificates." The severity of the flaw is also proved by the fact that

US-CERT released an alert about it, in which they also warned that the vulnerable Mozilla NSS library is often included in 3rd party software, including Linux distributions, Google Chrome, Google OS and others. Google has released a security update that fixes the bug for its Chrome stable channel, so Chrome users should update as well. Hopefully, patches for the other affected software will soon follow. More technical details about the flaw can be found here. The vulnerability has been reported both by Antoine Delignat-Lavaud, security researcher at Inria Paris in team Prosecco, and the Advanced Threat Research team at Intel Security. To read more click HERE

FBI warns of malicious insider threats increase

Heise Security, 25 Sep 2014: The FBI and DHS have issued a warning to businesses about the increase in security incidents involving malicious insiders (current or former employees, contractors, or other business partners). "The exploitation of business networks and servers by disgruntled and/or former employees has resulted in several significant FBI investigations in which individuals used their access to destroy data, steal proprietary software, obtain customer information, purchase unauthorized goods and services using customer accounts, and gain a competitive edge at a new company," they noted. "The theft of proprietary information in many of these incidents was facilitated through the use of cloud storage Web sites, like Dropbox, and personal e-mail accounts. In many cases, terminated employees had continued access to the computer networks through the installation of unauthorized remote desktop protocol software. The installation of this software occurred prior to leaving the company." There have also been a few extortion attempts where disgruntled or former employees attempted to extort money from their employer by modifying and restricting access to company Web sites, disabling content management system functions, and conducting DDoS attacks. The Bureau notes that security incidents involving insiders can cost the company a pretty penny, and have shared a set of recommendations for preventing such incidents from occurring within their organization. These include terminating employee access to accounts they don't need access to, terminating dismissed employees' or contractors' accounts immediately, changing any administrative passwords they had knowledge of, preventing employees from accessing cloud storage Web sites and downloading unauthorized remote login applications on corporate computers, and more. The official bulletin is available here. To read more click HERE

Consumers increasingly blame companies for data breaches

Heise Security, 25 Sep 2014: Moving forward, every company involved in a major data breach—those actually attacked, such as retailers Home Depot, Target, Goodwill and Neiman Marcus, as well as banks, healthcare, insurance and Internet Service Providers, etc.—is going to pay an even higher price when customers' information is compromised. In fact, each high-profile hack will take its toll on the executive suite and the bottom line alike, say the results of a poll conducted by HyTrust. The survey reveals that more than half of all respondents, 51%, will take their business elsewhere after a breach that compromises personal information, including address, social security number, and credit card details. Almost as many, 45.6%, say the companies involved should be considered 'criminally negligent' the moment a breach occurs, with the majority also believing that all officers of a company should be held responsible. More than a third, 34.2% believe the worst piece of information to be compromised is the social security number (SSN). These findings are significant as the issue of data security is all over the headlines… again. Just this month, retail giant Home Depot became the latest victim of a massive cyber-assault, and we now know it's potentially the largest retail security breach in history. The company acknowledged that a long-running, sophisticated hack with intrusions starting back in April using custom-built malware led to the theft of some 56 million credit and debit card numbers. That would mean it surpasses even the staggering losses accruing from the attack on Target late in 2013. That episode led to big changes in the executive suite; it remains to be seen what effect the newest revelations from Home Depot will have, but they are likely to be severe. "There probably isn't a single straw that broke the camel's back—it's just the sheer volume of stories about data breaches, many at companies that have developed a customer-friendly brand," said Eric Chiu, President at HyTrust. "What this poll shows is that companies are finally, and inevitably, being held to account for their security vulnerabilities. Consumers

have options, and when there are endless stories about the loss of confidential information, they're going to other vendors. Every security breach clearly has a direct impact on operations, but there's now clear evidence that there's extensive brand damage as well, and the executives involved will have to pay the price." Each question surveyed 2,000 respondents, offering a clear view into the evolving consumer mindset regarding this complex issue. For example:

- Once is enough: Most consumers (45.6%) blame the companies involved the moment a data breach occurs, while only 12% withhold condemnation until 'it happens more than once.' Additionally, this finger-pointing increases with age, with 34% of 25-34 year olds laying immediate blame verses 51% of those 65 and up. The more consumers make, however, the more forgiving they tend to be; the top answer for those making $150K or more shifted to 'when it happens more than once.' Blame is also more vehemently focused on a breached company, understandably, when a person's identity is stolen or misused.
- Income and gender matter: Higher earners are more concerned about their SSNs: 36.5% of those making $50k-$74 cite this potential theft as most serious, while that falls to 22.8% among those making $24k or less. Meanwhile, women (17.9%) are twice as likely as men (9.6%) to worry about the loss of family photos and mementos.
- Talking with their wallets: While 51% of respondents overall say they will take their business elsewhere following a data breach, that number jumps to 60.2% among consumers in the 35-44 age range. That finding, which focuses on a key demographic, should give retailers and other potential targets significant cause for concern.
- Chief Security Officers (CSOs / CISOs) take note: When asked who in particular should be held 'ultimately accountable' for failures in information security, 19.7% of respondents don't make a distinction between executives with varying responsibilities, pointing the finger at 'all officers' of a company. However, men and women aged 25-34 identify CSOs as most responsible, while those in the 45-54 age bracket go easiest on them.
- The Board gets off easy: A company's Board of Directors is ranked as the corporate entity most 'off the hook' in terms of accountability for a data breach.

To read more click **HERE**