THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

18 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

Chinese hacked U.S. military contractors, Senate panel finds

Reuters, 17 Sep 2014: Hackers associated with the Chinese government have repeatedly infiltrated the computer systems of U.S. airlines, technology companies and other contractors involved in the movement of U.S. troops and military equipment, a U.S. Senate panel has found. The Senate Armed Services Committee's year-long probe, concluded in March but made public on Wednesday, found the military's U.S. Transportation Command, or Transcom, was aware of only two out of at least 20 such cyber intrusions within a single year. The investigation also found gaps in reporting requirements and a lack of information sharing among U.S. government entities. That in turn left the U.S. military largely unaware of computer compromises of its contractors. "These peacetime intrusions into the networks of key defense contractors are more evidence of China's aggressive actions in cyberspace," Democratic Senator Carl Levin of Michigan, the committee's chairman, said in releasing the report. Officials with the Chinese embassy in Washington did not immediately comment. Cybersecurity expert Dmitri Alperovitch, chief technology officer with the security firm Crowdstrike, said China had for years shown a keen interest in the logistical patterns of the U.S. military. The investigation focused on the U.S. military's ability to seamlessly tap civilian air, shipping and other transportation assets for tasks including troop deployments and the timely arrival of supplies from food to ammunition to fuel. Those companies typically do not have the level of defense against hackers as major weapons makers or the military itself. In a 12-month period beginning June 1, 2012, there were about 50 intrusions or other cyber events into the computer networks of Transcom contractors, the 52-page report stated. At least 20 of those were successful intrusions attributed to an "advanced persistent threat," a term used to designate sophisticated threats commonly associated with attacks against governments. All of those intrusions were attributed to China. Senator Jim Inhofe of Oklahoma, the committee's top Republican, called for a "central clearinghouse" that makes it easy for contractors to report suspicious cyber activity. "We must ensure that cyber intrusions cannot disrupt our mission readiness," Inhofe said. The investigation found that a "Chinese military intrusion" into a Transcom contractor between 2008 and 2010 "compromised emails, documents, user passwords and computer code." In 2012, another intrusion was made into multiple systems of a commercial ship contracted by Transcom, the report said. To read more click **HERE**

September 16, KrebsOnSecurity – (National) **Breach at Goodwill vendor lasted 18 months.** Payment vendor C&K Systems stated that its hosted managed services systems were found by investigators to be compromised between February 10, 2013 and August 14, 2014, allowing the installation of the infostealer.rawpos point of sale (PoS) malware that led to payment card breaches from over 330 Goodwill retail locations. The malware infection was not detected by the company's systems until September 5 and affected Goodwill and two other customers. Source: http://krebsonsecurity.com/2014/09/breach-at-goodwill-vendor-lasted-18-months/

September 16, U.S. Securities and Exchange Commission – (International) **SEC charges IT employee at law firm with insider trading ahead of merger announcements.** The U.S. Securities and Exchange Commission September 16 charged a senior information technology professional at law firm Wilson Sonsini Goodrich & Rosati with allegedly engaging in insider trading using information from

client-related databases to make over $300,000 in illicit profits using a brokerage account held in the name of a relative in Russia. The U.S. Attorney's Office for the Southern District of New York also filed criminal charges against the man in a parallel action. Source: http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370542965393

September 17, Securityweek – (International) **Amazon fixes persistent XSS vulnerability affecting Kindle library.** Amazon addressed a cross-site scripting (XSS) vulnerability on the Amazon Web page used to manage users' Kindle libraries that could be used by an attacker to inject malicious code through eBook metadata. Source: http://www.securityweek.com/amazon-fixes-persistent-xss-vulnerability-affecting-kindle-library

September 17, Help Net Security – (International) **Macro based malware is on the rise.** Researchers with Sophos found that macro-based malware created in Visual Basic rose from around 6 percent of document malware to 28 percent in July, among other findings. Source: http://www.net-security.org/malware_news.php?id=2867

September 16, Threatpost – (International) **Adobe gets delayed Reader update out the door.** Adobe released new versions of Adobe Reader and Acrobat September 16 that were delayed during Adobe's scheduled patch release the week of September 8. The updates close eight vulnerabilities including two memory corruption issues and a cross-site scripting (XSS) vulnerability affecting Macintosh users. Source: http://threatpost.com/adobe-gets-delayed-reader-update-out-the-door

September 16, Threatpost – (International) **Archie exploit kit targets Adobe, Silverlight vulnerabilities.** Researchers at AlienVault Labs analyzed a new exploit kit first identified by EmergingThreats researchers and found that the Archie exploit kit attempts to exploit older versions of Adobe Flash, Reader, and Microsoft Silverlight and Internet Explorer. Source: http://threatpost.com/archie-exploit-kit-targets-adobe-silverlight-vulnerabilities

iOS 8 fixes bucketload of severe security bugs
Heise Security, 18 Sep 2014: Apple has released the latest version of its mobile OS on Wednesday, and in it has fixed over 50 vulnerabilities, many of which are very serious:

- Two vulnerabilities allowed a local attacker to escalate privileges and install unverified (likely malicious) applications
- A validation issue in the handling of update check responses allowed an attacker with a privileged network position to cause an iOS device to think that it is up to date even when it is not
- Two vulnerabilities in CoreGraphics made it possible for a maliciously crafted PDF file to terminate apps or execute arbitrary code
- Several vulnerabilities in the IOHIDFamily kernel extension made it posible for a malicious app to read kernel pointers, which can be used to bypass kernel address space layout randomization, or to execute arbitrary code with system privileges (the latter was also made possible by the existence of several IOKit bugs)
- A Libnotify bug allowed a malicious application may be able to execute arbitrary code with root privileges
- Two Safari vulnerabilities made it possible for attackers and websites to intercept or harvest user credentials
- 12 WebKit bugs could have been misused by attackers to execute arbitrary code on the device by simply creating a malicious website and tricking users into visiting it.
- With iOS 8, Apple has also updated its certificate trust policy and has randomised the MAC address to prevent potential device tracking attacks via passive WiFi scans.

To read more click HERE

Malicious eBay listings redirect users to phishing site

Heise Security, 18 Sep 2014: An IT worker from Scotland who is also an "eBay PowerSeller" has discovered an eBay listing for an iPhone that was rigged to redirect potential buyers to a spoofed eBay login page. Paul Kerr happened upon the listing by chance, and immediately recognized the redirection for what it was: a phishing attempt. At the time, the advert had been up for 35 minutes, he noted, and he immediately notified eBay of the problem. But, despite getting assurances that the matter will be dealt with immediately, the listing remained available for over 12 hours, Kerr claims. "They should have nailed that straight away, and they didn't," he commented. The malicious listing contained Javascript code that took advantage of a cross-site scripting (XSS) flaw in the website and, according to the BBC, there were in total three listing posted by the same malicious seller, and at least two contained the redirection code. All three listings have been removed by eBay, but its spokesman admitted the existence of only one. "We take the safety of our marketplace very seriously and are removing the listing as it is in violation of our policy on third-party links," he added. Chances are good that some people have fallen for this phishing scheme, but it's difficult to say what the exact number could be. This is not the first time that XSS vulnerabilities in the eBay website have been misused by malicious actors, and it probably won't be the last. To read more click HERE

72% of businesses don't trust cloud vendors

Heise Security, 17 Sep 2014: There is widespread mistrust of cloud providers across Europe with seven in 10 businesses accusing them of failing to comply with laws and regulations on data protection and privacy, according to Netskope and The Ponemon Institute. The study shows that 53% of respondents said the likelihood of a data breach increases due to the cloud, and the Ponemon Institute study also found that data breaches increase the expected economic impact by as much as three times when they involve the cloud. This phenomenon is known as the "cloud multiplier effect," and the research found this applies to varying degrees in accordance with different cloud scenarios, such as increased data sharing from cloud apps or increased use of mobile devices to connect to cloud. Using a previously established cost of €136 per compromised record, the loss or theft of 100,000 customer records would cost an organisation €13.6M. But when survey respondents were asked about the potential repercussions from increased usage of cloud services, their lack of trust pushes them to triple the probability of a data breach. Assuming an increase in cloud storage, the estimated probability of a data breach involving the loss or theft of high value information or intellectual property goes up by 126%. In addition, respondents perceived that simply increasing the use of any cloud services causes the impact of a data breach of the same type to go up by 159%. Finally, IT professionals concluded that rapid vendor growth and volatility of a cloud provider could increase the probability of a data breach involving the loss of 100,000 customer records or more by 108%. The research found widespread mistrust of cloud providers:

- In addition to the 72% of respondents indicating they believe that cloud providers fail to comply with data protection laws and regulations, 84% of respondents also doubted that their cloud service providers would notify them immediately if their intellectual property or business confidential information were breached
- 77% of those questioned claimed that their cloud providers would not notify their organisation immediately if they had a data breach involving the loss or theft of customer data.

64% of IT pros think that their organisation's use of cloud services reduces its ability to protect confidential information and 59% believe it makes it difficult to secure business-critical applications. In contrast, the majority of respondents still considered cloud to be equally secure or more secure than on-premises IT, which perhaps indicates more about their lack of confidence in their on-premises security tools than it does about their confidence in the security capabilities of cloud providers. "This study proves that some companies are struggling with shadow IT and need much more visibility into what data and

apps are being accessed in the cloud and guidance on how they should analyse vendors," said Sanjay Beri, chief executive officer and co-founder of Netskope. "We all know that cloud can offer productivity gains, but these shouldn't come at the expense of security. Our respondents agreed that cloud has the potential to be more secure than on-premises IT, but this is only true if they have policy enforcement capabilities coupled with deep contextual visibility into cloud transactions — especially those involving sensitive data." Comparing the results of this study with a previous Netskope and Ponemon Institute study, which investigated the cloud multiplier effect in the US, European organisations are more confident in their ability to secure the cloud. 51% of US respondents claimed that their organisation's effectiveness in securing data and applications was "low," double the percentage of European respondents who felt the same (25%). Likewise, 52% of European IT professionals rated their organisation's effectiveness as "high" but only 26% of US respondents agreed that their organisation was highly effective at securing data and apps in the cloud. To read more click **HERE**