THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

20 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

October 17, Threatpost – (International) **SAP patches DoS flaw in Netweaver.** SAP released a patch for its Netweaver platform that closes a remotely exploitable denial of service (DoS) vulnerability reported by Core Security researchers in June. The vulnerability could allow an unauthenticated attacker to use a specially crafted SAP Enqueue Server packet to create the DoS condition. Source: http://threatpost.com/sap-patches-dos-flaw-in-netweaver/108896

October 17, IDG News Service – (International) **New technique allows attackers to hide stealthy Android malware in images.** Two researchers presenting at the Black Hat Europe conference October 16 revealed a technique dubbed AngeCryption that could allow an attacker to hide malicious Android applications inside image files in order to avoid detection by antivirus programs and potentially the Google Play store's malware scanner. Source: http://www.networkworld.com/article/2835433/new-technique-allows-attackers-to-hide-stealthy-android-malware-in-images.html

October 16, Softpedia – (International) **XSS risk found in links to New York Times articles prior to 2013.** A student reported and published a proof of concept for a vulnerability in articles on the New York Times Web site published before 2013 that could allow attackers to hijack browser sessions, direct users to phishing sites, or steal cookies by exploiting a cross-site scripting (XSS) flaw. The vulnerability exists on pages containing certain buttons and does not affect the most recent versions of popular Web browsers. Source: http://news.softpedia.com/news/XSS-Risk-Found-In-Links-to-New-York-Times-Articles-Prior-to-2013-462334.shtml

October 16, The Register – (International) **Bad news, fandroids: He who controls the IPC tool, controls the DROID.** Researchers with Check Point presenting at the Black Hat Europe conference October 16 detailed a flaw in the Android inter-process communication (IPC) tool Binder that could allow attackers to override in-app security features to tamper with apps and steal passwords and other information. Source: http://www.theregister.co.uk/2014/10/16/android_messaging_mechanism_security_flawed/

October 16, IDG News Service – (International) **All-in-one printers can be used to control infected air-gapped systems from far away.** A cryptographer and two researchers from Ben-Gurion University presenting at the Black Hat Europe conference October 16 demonstrated how an all-in-one printer could be used to issue commands to infected systems on an air-gapped network by shining infrared or visible light at the scanner lid when open, issuing commands to malware already planted on the system via USB drive or other method. The researchers were able to successfully test the method at a target printer inside a building at 200, 900, and 1,200 meters and stated that a more powerful laser could produce reliable results from up to 5 kilometers. Source: http://www.networkworld.com/article/2834973/allinone-printers-can-be-used-to-control-infected-airgapped-systems-from-far-away.html

Beware of Ebola-themed phishing, malware campaigns and hoaxes

Heise Security, 17 Oct 2014: US-CERT released an advisory warning users about email scams and cyber campaigns using the Ebola virus disease as a theme. "Phishing emails may contain links that direct users to websites which collect personal information such as login credentials, or contain malicious attachments that can infect a system," they pointed out. They advise users to be careful when dealing with these types of email messages, and urge them not to follow links or open attachments contained in them. They advised them to keep their AV software up-to-date, and to refresh their knowledge about how to protect themselves from malicious email attachments and avoid social engineering and phishing attacks. Another, less immediate danger are online hoaxes. Hoax-Slayer has compiled a pretty good list of current Ebola-related ones, including the one that claimed that a number of iPhone 6 phones have been contaminated with Ebola during manufacture and are helping the virus to spread. "Sharing false information about Ebola is both dangerous and irresponsible," he noted, and added that "criminals are also getting in on the act by peddling useless Ebola remedies and using Ebola as a cover story for advance fee scams." To read more click HERE

Apple releases MEGA security patch round for OS X, Server and iTunes

TheRegister, 17 Oct 2014: While the world+dog was distracted by all the shiny new iThings Tim Cook was showing off on Thursday, Apple quietly puMPED out patches for 150 CVE-issued bugs in its server and desktop operating systems and the iTunes media player. The newly released OS X Yosemite, version 10.10, includes a fairly hefty patch load, more so than most other operating systems at launch. In all there were 45 CVE patches for the new OS, and some pretty major flaws fixed. There's a similar set of updates for OS X Mountain Lion (10.8.5) and OS X Mavericks (10.9.5). Bash gets a patch to fix Shellshock and SSL 3.0 support also gets attention to fix the POODLE (Padding Oracle On Downgraded Legacy Encryption) flaw in its operating system. But there are a host of other serious fixes, such as the ability to brute-force the PIN for Find My Mac, dodgy Wi-Fi and Bluetooth security, and a host of remote-code execution flaws. But it was iTunes that got the biggest patch load – 83 of the things that were deemed worthy of fixing in Apple's somewhat bloated media player. Of the patched iTunes flaws, Google discovered 31, with Apple managing 30, and two patches coming from a combined effort from both companies: that's due to Google finding vulnerabilities in WebKit; there's a certain amount of software crossover between the two companies. Elsewhere are patches for OS X Server versions two, three and four, with the latter getting the bulk of fixes with 18 CVE patches, which the two prior builds got one apiece. Mountain Lion and Mavericks also got a security update in this patch cycle. To read more click HERE

US government fines Intel's Wind River over crypto exports

TheRegister, 17 Oct 2014: The US Government has imposed a $750,000 fine on an Intel subsidiary for exporting encryption to China, Russia, Israel and other countries Wind River Systems was fined for exporting products that incorporated encryption to foreign governments and to organizations on the US government restricted list. The controversial move means the US Department of Commerce appears to be coming down heavily against the export of encryption even in cases where no export to sworn enemies of the US (Iran, Cuba and North Korea etc.) is involved. The Intel subsidiary was fined for falling to get Department of Commerce licenses for a modest piece of business, valued at under $3m. As such the fine represents a slap on the wrist, but it's still a clear signal that priorities are changing. Previously self-reported cases of crypto export used to be handled by a warning only. Multinational commercial law firm Goodwin Procter warned its clients to treat what happened to Wind River as the new normal. Wind River Systems exported its software to China, Hong Kong, Russia, Israel, South Africa, and South Korea. BIS [Bureau of Industry and Security] significantly mitigated what would have been a much larger fine because the company voluntarily disclosed the violations. We believe this to be the first penalty BIS has ever issued for the unlicensed export of encryption software that did not also involve comprehensively sanctioned countries (e.g., Cuba, Iran, North Korea, Sudan or Syria). This suggests a fundamental change in BIS's treatment of violations of the encryption regulations. Historically, BIS has resolved voluntarily

disclosed violations of the encryption regulations with a warning letter but no material consequence, and has shown itself unlikely to pursue such violations that were not disclosed. This fine dramatically increases the compliance stakes for software companies — a message that BIS seemed intent upon making in its announcement. Senior FBI and US government law officers have repeatedly complained over recent weeks about plans by Apple and Google to incorporate enhanced security into smartphones. Now, as Techdirt notes, the conflict between government regulation and the tech industry is moving onto the renal original turf of the first crypto wars of the late 90s - the export of strong encryption. Strong cryptography was classified as a weapon and subject to export controls back in the 90s. This approach fell into disfavour for several good reasons that are even more relevant today than they were 20 years ago. Firstly cryptography is essentially applied mathematics and the knowledge is already out there. Secondly decent cryptography is a fundamental component of any computing system that aspires to be secure. This includes an increasing number of consumer devices with built-in processor chips, covering everything from smart-meters to electronic car locks and insulin pumps. Encryption is one of the best ways to safeguard against these devices getting hacked. Clamping down on the export of cryptography creates a huge competitive disadvantage for US tech companies trying to offer products and services worldwide. Foreign competitors, most likely from China, will inevitably step in and fill the breach. If the Snowden revelations hurt US-based cloud providers then what effect is stymying the US tech industry as a whole likely to have? At best the tougher line is an extra bureaucratic burden? In a statement, BIS provided an essentially bureaucratic justification for its enforcement action - Wind River had failed to apply for an export permit. Wind River Systems "voluntarily disclosed that between 2008 and 2011 the company made 55 exports of operating software valued at $2.9 million to governments and various end users in China, Hong Kong, Russia, Israel, South Africa, and South Korea. The operating software is controlled under Export Administration Regulations for national security reasons, and some of the export recipients in China are on the BIS Entity List." To read more click **HERE**

Oz privacy comish says breaches could double this year

TheRegister, 20 Oct 2014: The office of Australia's Federal Privacy Commissioner has received 60 voluntary data breach notifications in the six months since 12 March compared to 71 received in the 2014 financial year. The statistics provide to Vulture South and repeated at the Australian Information Security Association conference include all manner of consumer and staff privacy exposures including hacking breaches and lost storage devices. The data shows about 30 breaches have been noted since June 30. "Our office has been very busy over the last few months with data breaches voluntarily reported to us and some" discovered by the department", Commissioner Timothy Pilgrim told delegates at the conference last Friday. "In one instance we found out about a breach that happened three years ago and this is simply not acceptable and was clearly not going to be looked upon favorably by our office." Organizations whose breaches were reported by whistle blowers or more often the media could "pretty much rely on a full investigation being opened which may become a public process", Pilgrim told El Reg. The soon-to-be-shuttered Office of the Australian Information Commissioner (OAIC) processed all of the reported breaches since most did not require in-depth investigation. The absence of further scrutiny is a reflection of the affected organizations being found to have taken "reasonable steps" to secure private information before or after the event. Individuals impacted by the breaches had also been notified. Last year the OAIC received 4239 privacy complaints, a whopping 183 percent up on the previous 12 months. Its inquiry line fielded 11,000 calls and 2500 frustrated letters, up 30 percent. Most of these were from individuals. Pilgrim took the opportunity to tout the benefits of a mandatory data breach law, the mean sister of Australia's reformed Privacy Act which would compel organizations to report breaches and bolster security rather than purchase brooms and rugs. "I've always personally been in favor of a mandatory data breach notification system, as I believe it helps individuals to manage the risk to them in cases where their personal information has been compromised. "Data breaches unfortunately appear to be an inevitable part of business in the information age and a data breach notification law could help businesses deal with this risk and respond to this breach." To read more click **HERE**

South Korean ID system faces overhauls following 10 years of data thefts

Sophos Security, 15 Oct 2014: The South Korean government is considering reissuing national identity card ID numbers for every citizen over the age of 17, at the cost of billions of US dollars. The extreme step, reported by Associated Press, comes after a series of attacks that have left around 80% of its population at the mercy of hackers. The ID numbers and other personal data of an estimated 40 million of the country's 50 million citizens have been stolen from credit card companies, social networks and online gamers since 2004. The country's ID system, implemented in 1968, is a staple of South Korean life. The cards are required to register online accounts, take advantage of government services, get a job and even buy cigarettes. Unfortunately, the way in which the 13 digit ID numbers are formulated make them easy to steal as they are all constructed in the same way, using numbers based upon the citizen's date of birth, sex, place of birth and a sequential number used to identify those of the same sex who were born on the same day in the same location, as well as a check digit. Resident registration numbers' usage across different sectors made them 'master keys' for hackers to open every door and steal whole packages of personal information from unassuming victims. Even if their numbers are leaked, people are unable to change them, so hackers are constantly trying to obtain these numbers and are managing it easily. The country's president Park Geun-hye, who herself has fallen victim to data theft, called for a change in the current ID system in January and ordered a study of the available options which should be concluded before the end of the year. According to Kim Ki-su, a director at Seoul's Ministry of Security and Public Administration, the introduction of a new ID system, including the reissue of cards and new government systems, would cost a minimum of 700 billion won ($6.57 billion/£4.13 billion). He estimated that the cost to businesses, who may need to adjust their systems, could run into the trillions of won. ID number theft has become so prevalent in the country, in fact, that six men recently arrested for trading details told police they received only 1 won (less than one tenth of a cent) for each record they sold. I'm sure the people of South Korea, where over 85% of the population have internet access, will welcome any moves that see security catch up with technology. To read more click **HERE**

Commerce IG: Cloud service contracts lack needed clauses, security standards not met

Fierce Government IT, 20 Oct 2014: A review of cloud computing services in the Commerce Department found missing clauses in contractors' agreements to permit reviews of their facilities and operations, as well as lack of compliance with federal security standards. In examining a sample of cloud service contracts from three bureaus, the department's inspector general found that four did not contain a specific Commerce Department clause that would allow its investigators access to the provider's facilities, installations, operations, documentation, databases and personnel that would be used to perform such services. As a result, the IG would not be able to conduct inspections, investigations, audits and other reviews. Additionally, one contract did not contain a Federal Acquisition Regulation clause that would permit the agency access to a service provider's installations, documentation, records and databases, which is needed to make sure that government data remains secure and confidential, according to an IG memo dated Oct. 14 (**pdf**). The federal government leadership is being challenged to cut spending and reinvest in areas with greater opportunity. Another problem stated in the memo to top Commerce Department officials found that only two of the cloud services associated with the six IG-reviewed contracts used the Federal Risk and Authorization Management Program, or FedRAMP, which essentially provides baseline security standards for cloud services. "Nevertheless, all cloud services associated with the contracts we reviewed have been granted authorization to operate by the respective bureaus," the memo said. "As a result, bureau authorizing officials should be aware of risks associated with employing the cloud services that do not meet FedRAMP requirements." The IG reviewed a non-statistical sample of six contracts from the Census Bureau, the National Institute of Standards and Technology, and the National Oceanic and Atmospheric Administration. The department agreed with the IG's findings and said it would implement the memo's recommendations of including the contractual clauses and ensuring FedRAMP compliance. The IG review itself stems from a larger government-wide review initiated by the Council of Inspectors General on Integrity and Efficiency, which requested agency IGs about a year ago to review their cloud service contracts and FedRAMP compliance. A larger report on the state of cloud service

contracts across 20 participating federal agencies is being prepared. For more: - read the Commerce Department IG memo (pdf). To read more click HERE