THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

3 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

JPM Denies Report of Second Hack, Says 76M Customers Affected in Earlier Attack

Fox News, 2 Oct 2014: Morgan Chase (JPM) refuted a report Thursday afternoon that it experienced an attack on its systems for the second time in about three months. A spokesperson for the bank told FOX Business the report from the New York Times citing several people familiar with the situation is "false; we are not aware of any new cyber attack." The report from the Times suggested hackers with links to Italy or southern Europe gained access to the bank's servers, but didn't make clear whether the incident was a whole new attack, or whether more information was coming to light about a breach that happened earlier in the year. Late Thursday afternoon, JPM revealed that the earlier data breach, which took place in July, affected 76 million households and 7 million small businesses. But the bank said there's no evidence that account information for affected customers -- such as passwords, Social Security numbers and actual account numbers -- had been stolen. It also said it hadn't detected any fraudulent activity related to the hack. The Times issued a correction to its original headline Thursday afternoon clarifying "the article misstated the extent of the cyber security issues at JPMorgan Chase." In August, the nation's biggest bank by assets said it was investigating a possible cyber attack that happened in July and allowed hackers to enter many of the bank's servers. It was reported JPM and four of the nation's other big banks were the targets of coordinated attacks. Stolen in the breach were large amounts of data including checking and savings account information. Since news of the original attack broke, JPMorgan has worked with law enforcement officials to determine exactly how far the attack spanned, and taken steps to safeguard confidential information. At that point, the bank said it hadn't identified unusual fraudulent activity. To read more click **HERE**

Hackers Have Found A Flaw In Macs via Reddit

Business Insider, 3 Oct 2014: Criminals have discovered a flaw in OS X, the Mac operating system, and are using it to control thousands of Apple computers around the world. The Russian security company Dr. Web first discovered the software, known as "Mac.BackDoor.iWorm." We don't yet know how the software spreads, but Dr. Web has released information on the clever way it connects to the criminals who control the program. When a Mac is infected with Mac.BackDoor.iWorm, the program tries to make a connection to a command server. The iWorm reportedly uses Reddit's search function to find comments left by the criminals in a Minecraft discussion section of the site. (Minecraft is the block-building video game published by independent publisher Mojang, which Microsoft purchased for $2.5 billion in September.) After iWorm finds the Reddit comments, it attempts to connect to the server addresses listed in the Minecraft subreddit. Once connected, criminals can send commands to their "botnet" of infected computers. Botnets are often used to send spam emails, mine Bitcoin, or flood websites with traffic that eventually crashes them. It doesn't seem like the infected computers are currently being used for any attack, so the criminals behind iWorm are probably only growing the network for now. Dr. Web has published the number of computers that it believes have been affected by iWorm. As of last Friday, 17,658 infected Mac computers have been discovered, with 4,610 of them in the US. http://finance.yahoo.com/news/hackers-found-flaw-macs-using-121808264.html To read more click **HERE**

States worry about ability to hire IT security pros

Computerworld, 3 Oct 2014: States' efforts to improve cybersecurity are being hindered by lack of money and people. States don't have enough funding to keep up with the increasing sophistication of the threats, and can't match private sector salaries, says a new study. This just-released report by Deloitte and the National Association of State CIOs (NASCIO) about IT security in state government received responses from chief information security officers (CISO) in 49 states. Of that number, nearly 60% believe there is a scarcity of qualified professionals willing to work in the public sector. Nine in 10 respondents said the biggest challenge in

attracting professionals "comes down to salary." But the problem of hiring IT security professionals isn't limited to government, according to Jon Oltsik, an analyst at Enterprise Strategy Group (ESG). In a survey earlier this year of about 300 security professionals by ESG, 65% said it is "somewhat difficult" to recruit and hire security professionals, and 18% said it was "extremely difficult." "The available pool of talent is not really increasing," said Oltsik, who says that not enough is being done to attract people to study in this area. Oltsik's view is backed by a Rand study, released in June, which said shortages "complicate securing the nation's networks and may leave the United State ill-prepared to carry out conflict in cyberspace." The National Security Agency is the country's largest employer of cybersecurity professionals, and the Rand study found that 80% of hires are entry level, most with bachelor's degrees. The NSA "has a very intensive internal schooling system, lasting as long as three years for some," Rand reported. Another way to help security efforts, said Oltsik, is to seek more integrated systems, instead of lot of one-off systems that require more people to work on them. To read more click **HERE**

October 1, Threatpost – (International) **Schneider Electric fixes remotely exploitable flaw in 22 different products.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory to operators of 22 different Schneider Electric industrial control systems products after a researcher identified a remotely exploitable directory traversal vulnerability that could allow attackers to bypass Web server authentication and gain administrator access and control over devices. Schneider Electric released a firmware update to close the vulnerability in the products deployed in the manufacturing, energy, water, communications, and other sectors. Source: http://threatpost.com/schneider-electric-fixes-remotely-exploitable-flaw-in-22-different-products

October 1, Los Angeles Times – (California) **Cedars-Sinai says number of patient files in data breach much higher.** Cedars-Sinai Medical Center in Los Angeles notified 33,136 patients September 11 that their personal and health information may have been accessed after a password-protected, unencrypted laptop was stolen from an employee's home during a June burglary. The hospital previously reported the theft to 500 patients in August, but forensic analysis determined the laptop contained information for thousands of additional patients, including about 1,500 Social Security numbers. Source: http://www.latimes.com/business/la-fi-cedars-data-breach-20141002-story.html

October 1, KSTU 13 Salt Lake City – (Utah) **Provo City School District warning employees of data breach.** The Provo City School District in Utah notified about 1,400 employees that their personal information may have been compromised in a phishing attack September 29 that targeted an employee's email account which contained files of sensitive and personal employee information. The school district neutralized the breach and continues to investigate the scope. Source: http://fox13now.com/2014/10/01/provo-city-school-district-warning-employees-students-of-data-breach/

October 2, Securityweek – (International) **VMware releases software updates to fix ShellShock bug.** VMware released patches for several of its products in order to close the Shellshock vulnerability in GNU Bash. Source: http://www.securityweek.com/vmware-releases-software-updates-fix-shellshock-bug

October 2, The Register – (International) **Researchers bypass Redmond's EMET, again.** Researchers with Offensive Security reported that they were able to bypass the fifth version of Microsoft's Enhanced Mitigation Experience Toolkit (EMET) security tool on several versions of the Windows operating system. Source: http://www.theregister.co.uk/2014/10/02/researchers_bypass_redmonds_emet_again/

October 1, The Register – (International) **Bash bug flung against NAS boxes.** FireEye researchers warned that attackers are attempting to exploit the Shellshock vulnerability in GNU Bash in order to compromise Network Attached Storage (NAS) systems before the systems can be patched. The researchers reported that NAS systems made by QNAP were especially targeted and that attackers were seeking to install backdoors. Source: http://www.theregister.co.uk/2014/10/01/sheelshock_nas_attack/

October 1, Threatpost – (International) **Joomla re-issues security update after patches glitch.** The developers of Joomla released a second version of a security update October 1 after an initial update designed to close critical vulnerabilities created some technical issues with users. Source: http://threatpost.com/joomla-re-issues-security-update-after-patches-glitch

California toughens breach notification law

Heise Security, 1 Oct 2014: California Governor Edmund Brown has signed on Tuesday new legislation that will strengthen privacy and consumer protections in the state. The new set of bills will, among other things, require each state agency and department to conspicuously post its privacy policy on its website, and companies to offer identity theft prevention and mitigation services to consumers following data security breaches. "If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information," it is defined. The latter bill also addresses what form a breach notification must take, what it must include, and when it must be sent out and to whom. It's also interesting to note that it applies only to breaches in which unencrypted personal information is believed to have been compromised. This bill doesn't apply to providers of health care, health care service plans, or contractors regulated by the Confidentiality of Medical Information Act; financial institutions subject to the California Financial Information Privacy Act; entities governed by the medical privacy and security rules issued by the federal Department of Health and Human Services under the Health Insurance Portability and Availability Act (HIPAA); entities that obtain information under an agreement pursuant to the Vehicle Code; and businesses that are regulated by state or federal law providing greater protection to personal information than that provided by this law. To read more click **HERE**

Mayorkas: DHS in 'dire need' of cyber legislation

Fierce Government IT, 2 Oct 2014: A Homeland Security Department official said the department is in "dire need" of legislation that would address cyber threat information sharing and help it build its cybersecurity workforce. "We are not without tools, but we do have a dire need for legislation to better equip us," said Mayorkas, during an Oct. 1 Washington Post event. While recent cyber legislation – the Cybersecurity Information Sharing Act of 2014, or CISA, (S.2588) and the Cyber Intelligence Sharing and Protection Act, or CISPA, (H.R. 624) – has stalled on the Hill, Mayorkas said even without legislation, the department is "not without resource" or "without opportunity" to improve information sharing, cyber hygiene and private-sector collaboration. Mayorkas said the department also needs help hiring the right cybersecurity professionals. While DHS's cyberscueity mission is a compelling one, it still has a difficult time competing with the private sector to hire top-notch IT professionals "because of financial realities," he said. In May, Sen. Tom Carper (D-Del.) introduced a bill (S.2354) that would grant the secretary of DHS hiring and compensation authorities for cybersecurity comparable to those granted to the secretary of Defense. If passed, DHS would be enabled to hire at the same speed and with salaries comparable to those at DoD. The Homeland Security secretary would be permitted to establish positions, make direct appointments, set rates of basic pay, and provide additional compensation, benefits, incentives and allowances – such as retention bonuses – says the bill. A similar provision was included in a House bill (H.R.3696), which was introduced by Rep. Michael McCaul (R-Texas) in December 2013 but hasn't progressed much further since. To read more click **HERE**

SEC audit reveals lapses in laptop inventory, possibly affecting more than 1,000 computers

Fierce Government IT, October 1, 2014: An internal investigation found that the Securities and Exchange Commission must take more action to better track agency-issued laptop computers. In the audit (pdf) dated Sept. 22, the SEC inspector general said that the Office of Information Technology's inventory failed to include current locations of machines from an operations center that closed last year. The inventory also had incorrect locations for about 17 percent of the 488 laptops reviewed, incorrect user information for 22 percent of them, and could not account for 24 machines, the audit found. Additionally, the IG said that at least 88 asset management branch workers could delete asset records from the IT Service Management inventory database. "These weaknesses existed because personnel did not always understand their roles and responsibilities, and related policies and procedures were inadequate, had not been effectively communicated, and were not consistently followed," the report said. Extrapolating its findings to the larger pool, the IG estimated that the SEC's IT inventory could reflect inaccurate information on more than 1,000 laptops. To remedy the problems, the IG recommended that the IT office revise and communicate comprehensive procedures for maintaining laptop inventories that include clearly defined roles and responsibilities, managers' expectations for maintaining an accurate count, and guidance on when inventory updates are required. The IG also suggested that workers in the Computer Security Incident Response Center be given the ability to search for and track missing laptops using commercially available tools. They should also report periodic status updates on lost or stolen machines, the report said. Additionally, the IG recommended that the SEC complete its ongoing inventory to get a complete picture. To better control access to the inventory system, the IG said the agency should replace it with one that includes segregation of duty controls, minimizes the number of user accounts that have permission to delete assets from the inventory, and includes an audit trail. This review is a follow up to a March 2008 IG report, which found that the SEC's property management guidance did not identify laptops as sensitive property and the IT office had not done an agencywide baseline inventory of laptops since 2003. Those problems have been addressed, the current report said, but added that further improvement is needed To read more click **HERE**