THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

26 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

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

September 25, Softpedia – (International) **Bash bug "Shellshock" is as large as issue as Heartbleed.** A researcher found a security vulnerability in the GNU Bourne Again Shell (Bash) command interpreter named Shellshock available through versions 1.14 and 4.3 and used in several Unix-based operating systems such as Linux and Mac OS X that poses the risk of remote code execution and can be executed in many ways by applications. A patch was issued for the vulnerability CVE-2014-6271 but remained incomplete, and a second vulnerability, CVE-2014-7169, that was issued as a result remains unpatched. Source: http://news.softpedia.com/news/Bash-Bug-Shellshock-Is-As-Large-An-Issue-As-Heartbleed-459913.shtml

September 25, Securityweek – (International) **Critical signature forgery flaw found in Mozilla NSS crypto library.** Mozilla released an update for its products and Google updated Chrome and Chrome OS to address the "BERserk" vulnerability exposed by two independent researchers from Intel Security Advanced Threat Research Team and INRIA Paris-Rocquencourt who found that the Mozilla Network Security Services (NSS) cryptographic library can be exploited for signature forgery acts. The hackers can leverage the flaw in the parsing of ASN.1 encoded messages which use Basic Encoding Rules (BER) by exploiting the fact that the length of a field in BER can be made to use many bytes of data. Source: http://www.securityweek.com/critical-signature-forgery-flaw-found-mozilla-nss-crypto-library

September 24, Threatpost – (International) **More trouble for jQuery as second compromise reported.** JQuery, an open source JavaScript library, worked to mitigate a second compromise after its site's homepage was defaced. Representatives announced that the Web site was taken down and cleaned of infected files and that the company is working on re-securing its servers, and working to address vulnerabilities. Source: http://threatpost.com/more-trouble-for-jquery-as-second-compromise-reported/108510

September 24, Securityweek – (International) **SMB employees targeted with fake termination emails: Bitdefender.** Researchers at Bitdefender warned employees and IT administrators of small and medium-sized businesses about a rash of fake emails claiming false termination that is designed to distribute information-stealing malware using an ARJ file archiver. Once the attached file is decompressed and executed, the malware opens a clean rich text format (RTF) document which connects to attackers who execute instructions to the victim. Source: http://www.securityweek.com/smb-employees-targeted-fake-termination-emails-bitdefender

September 24, Network World – (International) **Apple yanks buggy iOS 8 update.** Apple pulled its iOS 8.0.1 update and is working on a patch after reports that the update was cutting off cell service and making the Touch ID fingerprint sensor inoperable. Source: http://www.networkworld.com/article/2687496/smartphones/apple-yanks-ios-8-update.html

September 24, Boulder Daily Camera – (National) **Jimmy John's confirms data breach at 216 shops, including in Longmont, Broomfield.** Jimmy John's Gourmet Sandwiches officials confirmed September 24 that stolen credentials were used by an undisclosed party to remotely log into the point-of-sale systems of about 216 of the company's stores nationwide between June 16 and September 5. Officials reported that breach affected transactions in which payment cards were swiped at the stores, and has since been contained. Source: http://www.dailycamera.com/boulder-business/ci_26596775/jimmy-johns-confirms-data-breach-at-216-shops

Flaw in Mozilla Network Security Services Allows Creation of Forged Certificates
Softpedia, 25 Sep 2014: A vulnerability in Mozilla's Network Security Services (NSS) cryptographic library could permit forging RSA certificates. NSS is a set of libraries that can be used to develop client and server applications with support for different secure communication protocols, like SSL, TLS or PKCS. The glitch would permit a potential attacker to create fake RSA certificates that are used to ensure communication with a legitimate server through digital signatures. Users risk landing on malicious websites Cybercriminals can use a fraudulent certificate to set up malicious websites that appear legitimate to the user. All the signs of a secure connection would be available, but at the other end, all information (credentials, sensitive financial details) entered by the user is collected by the crooks. Fake certificates can be used in phishing attacks, where the malicious website impersonates the original one. "Users on a compromised network could be directed to sites using a fraudulent certificate and mistake them for legitimate sites. This could deceive them into revealing personal information such as usernames and passwords. It may also deceive users into downloading malware if they believe it's coming from a trusted site," says Daniel Veditz, lead security researcher at Mozilla. Mozilla has already developed a patch for the vulnerability and proceeded to push it to its clients' products. At the moment, there are updates for multiple Firefox revisions on different platforms: Firefox 32.0.3, Firefox for Android 32.0.3, Firefox for Android 31.1.1, Firefox ESR 31.1.1 and Firefox ESR 24.8.1. The Thunderbird email client (build 31.1.2 and 24.8.1) and SeaMonkey (version 2.29.1) also benefit from the patch. Mozilla says that less stable editions of the web browser (Beta, Aurora) have also received the fix. Getting the latest version of the browser should be done automatically, through the built-in update mechanism. However, if the auto-update is disabled, the new versions are available straight from the developer. Users working with the Network Security Services library set are advised to get the latest revisions (3.16.2.1, 3.16.5 and 3.17.1) that contain the patch. Security researcher Antoine Delignat-Lavaud from team Proseco has been credited for reporting the issue in NSS that allowed a type of signature forgery attack. The flaw consists in "lenient parsing of ASN.1 values involved in a signature." Intel Security made the same discovery, independently, and contacted the Mozilla Security team; they dubbed it BERserk. Mike Fey from Intel-owned McAfee explained in a blog post that "ASN.1 messages are made up of various parts that are encoded using BER (Basic Encoding Rules) and/or DER (Distinguished Encoding Rules). This attack exploits the fact that the length of a field in BER encoding can be made to use many bytes of data. In vulnerable implementations, these bytes are then skipped during parsing." To read more click **HERE**

Kevin Mitnick Enters Zero-Day Brokerage Business
SoftPedia, 26 Sep 2014: Kevin Mitnick, the notorious black-hat hacker of the 90s turned security consultant after serving four and a half years in prison for computer and wire fraud, expanded the activity of his company through trading premium zero-day exploits, the price starting from $100,000 / €78,500. Named "Mitnick's Absolute Zero-Day Exploit Exchange," the exploit brokering service offers zero-days developed in-house or purchased from third parties, and sells them to customers, who have to comply with strict standards. Zero-day exploits take advantage of vulnerabilities that are unknown to the vendor of the targeted product, and no patch exists for them. In the wrong hands, they are highly dangerous as malicious actors could use them for nefarious purposes until the glitch is discovered and fixed. "We develop trust relationships and establish loyalty with our buyers and sellers to provide the safest platform for exploit exchange," says the announcement for the service, which functioned silently for half a year and only now became public. If the party is unknown to the company, they can be charged a fee at the

discretion of the firm to qualify to join. In an interview for Wired, Mitnick said that selling to criminal organizations or repressive regimes was out of the question. The service could be used by government agencies for targeted surveillance. "When we have a client that wants a zero-day vulnerability for whatever reason, we don't ask, and in fact they wouldn't tell us," Mitnick told Wired. Absolute Zero-Day is advertised as a closed network that functions based on referrals from trusted parties and provides exploits with a CVSS base score of at least 8 and have wide software distribution. Two programs are available, Absolute X and Absolute Z, the former allowing customers to retain exclusivity of the exploit for a certain period of time, for an agreed fee; the latter is more expensive and guarantees first knowledge of the availability of an exploit for a targeted system or product. Security experts can trade their zero-days through the service, details about their identity remaining confidential and the products being exposed to "top-paying government and corporate buyers." In order to cash in on their work, the exploit has to be validated and approved. Funds from the buyer are held in escrow in the meantime. Exploit brokerage services are not uncommon or illegal and there are multiple organizations that offer them. Vupen, Netragard, Exodus Intelligence are just a few of them. Mitnick's Absolute Zero-Day relies on the company's "unique positioning among security researchers and the hacker community" to intermediate the exchange between buyers and sellers. To read more click **HERE**

Phishers go after unprecedented breadth of targets

Heise Security, 26 Sep 2014: Apple is the most phished brand in the world, accounting for 17 percent of all phishing reports sampled and analyzed from the first half of 2014, say the results of the new Global Phishing Survey released by APWG. Apple's brand and associated marques, such as iTunes and iPad, eclipsed perennial phishing target favorite PayPal with the computing device manufacturer enduring 21,951 of the 123,741 phishing reports sampled. PayPal was the second most phished brand, targeted in 17,811 attacks, or 14.4 percent of the half's sample. The Chinese marketplace Taobao was third with 16,418 attacks, or 13.2 percent of the sampled attacks. "As the world's most valuable brand with a massive on-line user base, Apple has always been a phishing target, and with phishers concentrating more and more on online account takeover, consumers' Apple ID's are a tempting target," said Rod Rasmussen, President and CTO of IID and the survey's co-author. "As Apple provides more services and devices tied to one's Apple ID, including the just announced Apple Pay, it is no surprise that phishers are increasing their efforts to fool consumers into divulging their credentials, regardless of additional security measures Apple puts in place to protect their customers," Rasmussen said. The report found cybercrime gangs are aggressively pursuing brand diversity in their online fraud schemes, spoofing and otherwise leveraging the identities of some 756 institutions, the highest number the analysts had yet encountered. "If a site takes in personal data like passwords or credit card information, then phishers may want to exploit it," said Greg Aaron, President of Illumintel and the survey's other co-author. "We're seeing an unprecedented breadth of targets -- cloud storage sites, utility companies, business service providers, and real estate brokerages." Of the 87,901 domains used for phishing, the report identified some 22,679 domains, a quarter of the total sample, that the authors believe were registered maliciously by phishers. The number is primarily due to registrations by Chinese phishers, who prefer cheap (and free) domain name registrations in certain TLDs. The other 65,222 domains were almost all hacked or compromised on vulnerable Web hosting. To read more click **HERE**

SIS Cyber Threat to US under Debate

Darkreading, 23 Sep 2014: ICS/SCADA systems and networks hackable but not easily cyber-sabotaged without industrial engineering know-how, experts say.Amid fresh threats by ISIS against the US and its allies this week, worries of what the well-financed and social-media savvy militant group could do in the cyber realm has triggered debate over whether ISIS ultimately could or would disrupt US critical infrastructure networks. ISIS has made no specific threats to US critical infrastructure, and no one knows for sure whether the militant group has any plans for a cyber attack against US interests or even the technical capabilities to pull it off. Even so, US officials are keeping a watchful eye on ISIS' movements in the digital realm: NSA director Michael Rogers last week hinted that the agency is monitoring this. "We

need to assume there is a cyber dimension in every area we deal with," Rogers said in a speech at a Washington conference. Meanwhile, ICS/SCADA security experts dismiss dire predictions in some circles that ISIS -- or any other group -- could ultimately "take down" or significantly disrupt the US power grid via a distributed denial-of-service (DDoS) or other type of cyber attack. "The power grid isn't something you send a command to and it crashes. It has survived" nature and other events over the years, says Eric Byres, CTO and vice president of engineering at Belden's Tofino Security Products. "Even with the attack on the substation in Metcalf, Calif., the power stayed up," he says, referring to the bizarre April 2013 sniper attack there that took out 17 transformers. The power grid is highly distributed and built with Mother Nature's fickle whims in mind, with plenty of redundancy and backup. "What is often lost is that this industry understands in a real way what's resilient. They know there are going to be equipment failures, [and] Mother Nature," says Patrick Miller, founder, director, and president emeritus of Energysec.org. "It's virtually impossible to cause a widespread outage." Former US Department of Homeland Security counterterrorism official John Cohen says ISIS's preferred and flashy use of social media for recruitment, its graphic video productions of hostage executions, and its ability thus far to amass significant funding -- hundreds of millions of dollars by some estimates -- make ISIS a potential cyber attack threat. Cohen says he's not seen any information suggesting ISIS is targeting the US power grid. "I would be concerned if they were able to attract" cyber experts who could execute cyber attacks, says Cohen, who is chief strategy advisor at Encryptics. "From the standpoint of a security person, even if I don't have specific intel about a specific threat or plot underway, I have to look at all factors if I'm going to be prudent and establish the capacity to mitigate this type of threat." Concerns over ISIS's cyber capabilities recently were raised publicly by some former government officials. Peter Pry, executive director of the Task Force on National and Homeland Security, told multiple media outlets that ISIS has made contact with a major Mexican drug cartel that once took down a power grid in its native Mexico, and the US should prepare for such a threat. The ICS/SCADA community considers nation-states or other technically sophisticated attackers the main threat to industrial systems and plants. There are plenty of weaknesses in the security chain of ICS/SCADA environments, so hacking into an ICS system that runs centrifuges or other processing equipment is possible. But inflicting real damage on a plant, such as forcing centrifuges to slow or speed up dramatically, would require inside knowledge of the plant as well as plenty of engineering know-how, notes Dale Peterson, founder and CEO of Digital Bond. "What we see that's misunderstood is the engineering and automation skills needed to do real damage. We've seen these things are fragile and insecure … It's not difficult to gain access to many critical infrastructure systems -- a simple spear [phishing exploit] and pivot" can crash a control system, for instance, he says. But real physical damage would require engineering expertise, such as understanding how the targeted centrifuges operate, Peterson says. "But if you get the right team, with an engineer who understands how to program it, and a hacker, then it's not that hard to do" damage, he says. Renowned Stuxnet expert Ralph Langner says he doesn't believe ISIS would spend its time and money on cyber attacks against the US power grid when it appears to prefer more violent acts against people. Plus, the power grid would be less of a terror target than say, a chemical plant, which could potentially incur more physical damage and casualties, he says. Those sites are vulnerable to a sophisticated attacker, says Langner, founder of Langner Communications. There's a misconception in some of those sites that the safety logic in their systems protects against cyber attacks, he says. "That's nonsense," Langner says. A station controller system may be able to shut down a plant in a safe manner, but that doesn't mean it can't be hacked by a sophisticated nation-state actor, he notes. Craig Guiliano, senior threat specialist at security consultancy TSC Advantage, considers ISIS a legitimate cyber threat, pointing to reported claims of ISIS building a "cyber caliphate" and its own encrypted software. "They are pouring money into developing that type of cyber offensive capability," Guiliano says. "They have made good on their promises … If there's any group on the world stage where you have to take them at their word, it would be ISIS." The bottom line is that most software has flaws that attackers can exploit, and ICS/SCADA systems in power plants, manufacturing sites, and other utilities run vulnerable systems, security experts say. "Whether ISIS has the means to pull off something is an open question. What is clear is that fundamentally, all software can be hacked," says Andrew Ginter, vice president of industrial security at Waterfall Security. Some major

ICS/SCADA vendors are getting better about issuing fixes for software flaws, but the actual patching of ICS/SCADA systems remains the exception rather than the rule. Industrial plant operators are often hesitant to apply patches -- or make any software changes -- for fear of disrupting operations, which is the priority in manufacturing, power-plant generation, and other industrial environments. "Every change to software is a threat to safety and reliability" of the plant, Ginter says. Take Belden's Tofino Security, which four years ago offered a free upgrade to its Tofino Industrial Security System version 1.6 that included a security patch to all users -- even those not under a support contract -- who downloaded it within 30 days. "After 30 days, nobody was downloading it," recalls Belden's Byres, so the company reached out by email and added another 30 days to the offer. "It was super-frustrating for us," he says, after under a third of them ultimately downloaded it after two months. To read more click **HERE**

Disgruntled employees are increasingly e-sabotaging businesses, FBI says

Sophos Naked Security, September 25, 2014 Employees with an axe to grind are increasingly sticking it to their current or former employers using e-tools such as cloud storage sites or remote access to a company's computer network, the US Federal Bureau of Investigation and Homeland Security Department said on Tuesday. Such workers are using cloud storage tools such as Dropbox to steal trade secrets or proprietary software. Beyond that, the FBI says it's conducting a growing number of "significant" investigations into disgruntled and/or former employees who've used their network access to destroy data, obtain customer information, purchase unauthorized goods and services using customer accounts, or gain a competitive edge at a new company. In addition to cloud storage, personal email accounts are also being used to steal proprietary information. And in many cases, the FBI has found that terminated employees installed unauthorized RDP (remote desktop protocol) software before they exited their companies, thereby ensuring that they could retain access to the businesses' networks to carry out their crimes. Victimized businesses report that the costs of malicious insider cyber-sabotage range from $5000 to $3 million. It all adds up, given the value of stolen data, plus the costs of technology services, establishing network countermeasures, legal fees, loss of revenue and/or customers, and the purchase of credit monitoring services for employees and customers affected by a data breach. It's hard to pinpoint how much data loss can be attributed to malicious employees. For example, a report from the threat intelligence consultancy firm Risk Based Security (RBS) found that insider threat in 2013 was much less severe than many expected, with only 9.4% of data-loss incidents caused by malicious actions from insiders and 17.1% attributed to accidents. But that finding runs contrary to other studies. A year ago, Forrester Research found that 25% of survey respondents said that abuse by a malicious insider was the most common way in which a breach had occurred in the previous year. One thing seems to be certain: judging by what the agencies have reported, malicious insider threats are on the increase. Multiple incidents have involved disgruntled or former employees who've attempted to extort their employer by putting a chokehold on company websites, modifying and restricting access. In some cases, insiders have disabled content management systems or conducted distributed denial-of-service (DoS) attacks. As Naked Security has advised in the past, a sound course of action in dealing with security breaches, be they from malicious insiders, insiders who make mistakes, or outsiders, is to have an incident-handling plan in place before a breach takes place, rather than after. For example, a good incident-handling plan includes things such as the distribution of call cards, which could help in the event that normal communications are held hostage by a malicious insider who disrupts access to the LAN so that nobody can find anyone else's phone number and email. To read more click **HERE**

Home Depot breach totals: 56 million credit cards exposed, $62 million in losses

Sophos Naked Security, 19 Sep 2014: Lots of people who speculated about the source of the credit card data breach at the Home Depot turned out to be wrong. But those who suggested that Home Depot's breach might end up bigger than Target's turned out to be spot on. As the home improvement retail giant revealed in a statement on Thursday, 18 September 2014, 56 million unique payment cards were compromised in the attack. The attack on Target in late 2013 resulted in the theft of 40 million credit and debit card numbers, although Target also managed to lose 70 million other customer records. However,

despite some initial reports that malware responsible for the compromise of the Home Depot's point-of-sale (PoS) systems was the same malware that hit Target, that's apparently not the case. Instead, malware on the Home Depot's PoS registers was "unique, custom-built malware" that "had not been seen previously in other attacks," the company said. The malware had been present on Home Depot systems since April 2014 and was finally eliminated on 13 September 2014. The company said it began investigating the breach on 2 September 2014 after it was notified by banking partners and law enforcement of suspicious activity, and has worked with security firms and the US Secret Service to close off the attack. In response, the Home Depot has rolled out "enhanced encryption" in all of its US stores to make credit card data unreadable, and will complete adoption of EMV Chip-and-PIN technology by the end of the year. Canadian stores, which are already enabled with Chip and PIN technology, will receive the new encryption system in 2015, the company said. As is becoming routine in the wake of recent data breaches at Supervalu, The UPS Store and others, the Home Depot issued an apology and said it is offering free credit monitoring services to those affected. The company estimated that the cost of its investigation, credit monitoring, customer outreach, call center staffing and legal costs will add up to about $62 million, about $27 million of which it expects to have reimbursed by insurers. Yet the total cost of the breach could end up much, much larger. To read more click **HERE**