THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

29 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 26, Securityweek – (International) **Dyre malware takes inventory of software on infected systems.** Researchers from Proofpoint analyzed a new variant of the Dyre (also known as Dyreza) banking trojan and found that several new features were added to the malware, including the addition of its own SSL certification and a feature that enables hackers to collect cookies, client-side certificates, and private keys from an infected computer's Windows Certificate Store. The latest version of the trojan can also extract a list of installed programs and services from an infected computer to be by hackers to determine which vectors can be exploited in the future. Source: http://www.securityweek.com/dyre-malware-takes-inventory-software-infected-systems

September 26, Softpedia – (International) **Honeypot catches malware exploiting Shellshock Bash bug.** Alien Vault researchers found two pieces of malware through their honeypots, an Internet Relay Chat (IRC) bot and an Executable and Linkable Format (ELF) binary that offers malicious actors the possibility to use the infected machine in distributed denial of service (DDoS) attacks in order to exploit the Shellshock Bash vulnerability. Patches are available for several software platforms as attackers are rapidly working to exploit the CVE-2014-6271 vulnerability. Source: http://news.softpedia.com/news/Honeypot-Catches-Malware-Exploiting-Shellshock-Bash-Bug-460041.shtml

September 26, Macworld – (International) **Apple quickly issues iOS 8.0.2 update.** Apple released the iOS 8.0.2 patch which addresses several issues including reinstating improvements and flaws from the former update, iOS 8.0.1, that was promptly removed after it disabled Touch ID and cellular capabilities on the iPhone 6 and iPhone 6 Plus. Source: http://www.networkworld.com/article/2687736/security0/apple-quickly-issues-ios-8-0-2-update.html

September 26, Help Net Security – (International) **Phishers go after unprecedented breadth of targets.** The Anti-Phishing Working Group (APWG) released its Global Phishing Survey co-authored with Internet Identity (IID) and found that in the first half of 2014 Apple was the most phished brand in the world, accounting for 17 percent of all reports sampled. Paypal came in second accounting for 14.4 percent or 17,811 targeted attacks the report stated, among other findings. Source: http://www.net-security.org/secworld.php?id=17416

September 25, Securityweek – (International) **BlackEnergy malware linked to targeted attacks.** ESET and F-Secure researchers found that the BlackEnergy malware has been active in targeted attacks in 2014, modified to be used as a tool for sending spam and for online bank fraud. The alteration was dubbed "BlackEnergyLite" by researchers due to the lack of a kernel-mode driver component and less support for plug-ins and a lighter overall footprint. Source: http://www.securityweek.com/blackenergy-malware-linked-targeted-attacks

Cisco Lists 31 Products Vulnerable to the Shellshock Vulnerability
Softpedia, 29 Sep 2014: Cisco assessed the impact of the Shellshock bug on its products and compiled a list of 31 products vulnerable to the glitch that has been around for more than 20 years; a total of seven network solutions were deemed to be unaffected. On the list of devices that can be abused using the recently

discovered flaw in Bash, the company included products designed for network protection, connection routing, network management, voice and unified communications, as well as devices for collaboration and media content delivery and encoding. Among them are Cisco IronPort Encryption Appliance, Cisco GSS 4492R Global Site Selector, Cisco Mobility Services Engine, Cisco ACE Application Control Engine Module for the Cisco Catalyst 6500, Cisco Finesse, MediaSense, and Cisco TelePresence Serial Gateway Series. The product line from Cisco is still under scrutiny in order to determine other solutions that could be affected by the bug. Cisco assessed the Bash bug's severity using the latest version of the Common Vulnerability Scoring System (CVSS) and assigned a base score of 7.5 because the impact on its products is only partial. The CVSS score for Shellshock is 10 out of 10, having gained maximum points because of its complete impact on a system and easy exploitation. "The impact of this vulnerability on Cisco products varies depending on the affected product. Successful exploitation of the vulnerability may allow an unauthenticated attacker to run commands from the Bash shell," explains Cisco in a security advisory (link). Software updates mitigating the risk of compromise through Shellshock have been made available by the company, and customers are recommended to check with their maintenance providers for compatibility issues before deploying the fixes. Oracle is also facing trouble from Shellshock, initially listing 32 of its products as being vulnerable to the bug. In the meantime, the company changed the list and appended new products; it also included new ones on the list of solutions that benefit from a patch. Shellshock was disclosed publicly on Wednesday, September 24, and it is believed to be a bigger problem than Heartbleed. Applying the latest patches from the developers should be a priority for anyone with a vulnerable version of the Bash command interpreter for Linux. Several fixes have been developed and delivered to clients through updates because the first attempts to eliminate the glitch failed and opened the door for other exploitation methods. To read more click HERE

User Profiling Services Could Be Compromised for More Targeted Attacks

Softpedia, 29 Sep 2014: Marketing companies gather all sort of information based on the IP address used for visiting websites. Security researchers believe that the user profiling these organizations do could be leveraged by malicious actors for more efficient attacks. Targeted advertising has been honed up to such a degree that browsing for particular subjects is enough to generate targeted advertisements on visited websites and even to receive emails in connection to the matter of interest for the user. In one case, spotted by security researchers at F-Secure, an individual received an email with an offer for a plane ticket to San Francisco, only hours after having discussed with a friend over the phone purchasing one. Cybercriminals getting useful information about the potential victim from a phone conversation is unlikely; but the target in the case mentioned above could have searched for cheap plane tickets on various websites that recorded his interest and created a profile. This, on the other hand, could have revealed a match in the user profiling database of a service. Abusing such a database would provide cybercriminals with incredible details about potential victims, and instead of blindfoldedly sending spam messages in the hope of entrapping someone, they can devise emails that appear to respond to the current need of a user and thus increase the chances of compromising their computer. Evidence in support of this theory occurred after the security experts analyzed the sample email from the potential victim and discovered that the malware employed in the attack had only 1,250 instances in their sample database; this "would indicate that this particular malware is not being spammed to large audiences." The email received by the individual claimed to be an order notification from Delta Airlines, purporting to provide a plane ticket to San Francisco in the attachment. The file appended to the message has been identified by F-Secure as being a variant of Trojan.Krypt.AU. "So this case looks very much like some targeted advertising services were misused for victim discovery by malware authors. We have seen advertising misused a lot with search engines, but this is the first case where we have indications that e-mail advertising services would be used in similar manner," says F-Secure in a blog post. The researchers also admit that this could very well be just a weird coincidence, although abusing marketing profiling information is definitely worth keeping an eye on. To read more click HERE

Linux Kernel 3.17 Delayed by a Week, Linus Torvalds Is Not Happy

Softpedia, 29 Sep 2014: Linux Torvalds has grudgingly released a new Linux kernel RC in the 3.17 branch and promised that he would try to release the final version next week. Linux kernel 3.17 should have arrived this past weekend, but it looks like we're going to have to wait another week for that to happen. Nothing really stands out in this new build, but it wasn't good enough for a final release. Usually, Linus Torvalds, who is the maintainer of this branch, waits until he has a quiet week before releasing the stable version of the kernel. That obviously didn't happen. Delaying a kernel release to make sure that everything works as it should is a common occurrence in the development cycle. As it was to be expected, Linux Torvalds is not thrilled about delaying the release of the Linux kernel 3.17 for another week, but he feels that it was necessary. Users will have to wait for a few more days to get their hands on the new release. "So I was really hoping that I could have left rc6 as the last rc and just releasing 3.17 today, but that was not to be. It's not that anything particularly scary happened, but quite frankly, things just didn't calm down as I hoped for. And while my travel schedule would have made it really nice had I been able to just do a shorter-than-usual release, 'convenience' isn't really part of the release criteria." "Oh well. This will likely mean that (barring unforeseen circumstances) next weekend sees the 3.17 release, and then due to travel, I probably will just delay opening the merge window by a week after that. And I'll be very grumpy if people send me pull requests that I deem inappropriate at this point," says Linus Torvalds in the email. The Linux kernel 3.17 branch should provide some interesting new features, such as better Intel Broadwell support, a number of improvements for the open source version of the NVIDIA drivers, lots of Radeon enhancements, and much more. These are just a few of the features, but the final version will be quite a catch. To read more click **HERE**

Woman Takes Home iPhone 6 Loaded with Someone Else's Pictures

Softpedia, 29 Sep 2014: A woman going by the name of Mary Biondi bought an iPhone 6 from Sprint last week and wanted it activated. The staffer in charge with these services didn't do a very good job, to say the least. "[The employee] just said, 'I am really sorry. I did something really bad and someone else's information is on your phone'," Biondi says, according to KCRA. That's not the worst bit. The employee who made the mistake let Biondi leave the store with that person's information on her new iPhone. She was told to head to the Apple Store and have the device wiped clean, but the Sprint staffer had no guarantee that she'd do that. Apparently, Sprint wishes to offer the same setup services as Apple does, only the former fails to train its staffers properly. "I am still so shocked that they actually just let me leave with the phone and whatever information -- it was somebody else's," Biondi said. Major security concern According to the report, the man whose iCloud account trickled onto Biondi's iPhone was told that "there was a computer file that was supposed to be deleted over the weekend, but never was." Imagine if that was your iCloud account that Sprint loaded up on someone else's iPhone. Would you be able to sleep at night knowing that someone, somewhere can see your personal photos and videos, as well as access social networks posing as you? What's more worrying is that Sprint is allowed to keep iCloud accounts that they can just "forget" to delete. To read more click **HERE**

32 Oracle Products Do Not Have Patch for the Shellshock Bash Bug, Yet

Softpedia, 27 Sep 2014: Dubbed Shellshock, the GNU Bash bug currently affects a total of 35 products from Oracle, but only 3 of them have been provided with patches, leaving the rest of 32 vulnerable to attacks. The severity of the security flaw, which has been present in the default command line shell available for Linux for more than 20 years, is very high. On top of this, there are reports that the glitch is actively exploited in the wild. Shellshock can be exploited remotely by a malicious actor, as authentication is not required, to run arbitrary code on the affected system by adding malicious commands to variable functions passed by applications to Bash. "Oracle is still investigating this issue and will provide fixes for affected products as soon as they have been fully tested and determined to provide effective mitigation against the vulnerability," a security advisory from the company says (link). No date is given for the release of patches for the affected products, and there is no word on sending notifications to users once a fix becomes available, which means that customers have to monitor the Patch Availability Table in order to

learn about the update. Among the products vulnerable to Shellshock are solutions with thousands of dollars on their price tags, such as SPARC Supercluster systems or Exalogic. The products that benefit from a fix are Exadata, Oracle Linux (versions 4 through 7) and Oracle Solaris (versions 8 through 11). To read more click **HERE**

Industrial Control Systems Equipment Difficult to Patch against Shellshock Bug

SoftPedia, 26 Sep 2014: Updating industrial control systems (ICS) to eliminate the recently discovered vulnerability in Bash command shell for Linux is a challenge difficult to overcome because patches may not even be available. The concern regarding the Shellshock bug is mostly centered around unpatched web servers, which can be abused by attackers to serve malware, steal credentials or gain deeper access into the network of the target. However, the impact of the bug expands beyond this, to ICS equipment, SCADA in particular, running Linux versions that may not even support upgrades anymore. Updates in the case of ICS are often not an option Reid Wightman of Digital Bond, a company offering security assessment services for control systems, says that in the industry of embedded devices it is common practice for developers not to prepare for patching scenarios. "There is still an awful lot of embedded industrial control systems equipment being manufactured today which has no way to even apply update," he said in a blog post. The threat ICS running embedded Linux face is quite serious, because any utility reaching to the Bash command shell to execute commands is actually a potential attack vector. The Shellshock bug can be exploited by sending an environment variable to Bash, with trailing malicious code. When the variable is interpreted, the nefarious command is also executed. Apart from lacking the update possibility, some ICS equipment is used for long periods of time before the switch to a newer one is done, most of the times outliving the maintenance duration offered by the developer. Another issue with patching things up consists in the fact that turning off the equipment could result in huge losses. Wightman told Threatpost that for this reason, the update can be executed during the maintenance window of the industrial control system, which is scheduled with a specific frequency. "Many industrial components run Linux and use bash in a way that will be exploitable," Wightman said. "Industrially hardened network switches, and even some programmable logic controllers (PLCs) and remote terminal units (RTUs) will likely be affected," the researcher added. ICS and SCADA are generally air-gapped On the bright side, the possibility of an attack on these systems used in critical infrastructures is lower than in the case of a web server, mainly because they are secluded from the Internet. This does not mean that risks are eliminated completely. Successful attacks on air-gapped systems have happened before, Stuxnet being the most suitable example. To read more click **HERE**

Heatmiser WiFi Thermostats Leak WiFi Credentials

Softpedia, 24 Sep 2014: Digital thermostats from Heatmiser that offer control over WiFi have been found to be riddled with security flaws that could be leveraged by a potential attacker to gain access to the WiFi connection. A reverse engineer, Andrew Tierney, discovered the wealth of issues while reading about vulnerabilities of another, older product of the company, Netmonitor. He then decided to check other products and found the line of WiFi thermostats that can connect directly to the router and provide access to their functions from afar by forwarding port 8086 for control through a mobile app and port 80 for control through the web browser. WiFi SSID and password available in plain text In one of the cases, the researcher noticed that after logging into a device, he could also learn the username, password, WiFi Service Set Identifier (SSID) and password. This could be done by simply looking into the source code of the web page, as all the information was available in the clear. "When logged into one of the devices, the username, password, WiFi SSID and WiFi password are all filled into the form and can be viewed easily by examine the source of the webpage. There is really no excuse for this – it's lazy," he says in a blog post. No need for credentials to alter settings. The researcher went through all the configuration steps of the device and found that access to the thermostat's functions can be gained without inputting credentials in the device's control web page. The web page is built from multiple HTM files, and one of them (left.htm) provides access to the temperature controls regardless of the login state. Basically, all someone needs to do is type in the IP address and the faulty page (http://87.56.123.121/left.htm) and they can make

changes to the temperature. Finding the IP address is not too difficult since port 8086 seems to be common to Heatmiser's WiFi thermostats. The researcher says that by scanning for this port "we can be fairly confident that anything with this port open is one of their devices." Next, a verification of port 80 can be done to extract more information. More issues are present in these devices, as there is the possibility of cross-site request forgery (CSRF) attacks, which means that malicious requests can be inserted in a link to the device and the command is executed. Commands can range from altering the configuration to modifying the password. Tierney stopped testing the product after uncovering no less than nine security glitches that could be easily abused, and reported them to the manufacturing company, which said that they would notify customers to close port 80 on the WiFi Thermostat until a solution is provided. A tweet from the company confirmed that some glitches were found in their product. To read more click **HERE**

iPhone 6 Can Be Unlocked with Fake Fingerprints, Just like the 5S Model

Softpedia, 24 Sep 2014: The Touch ID security technology implemented in the new iPhone 6 models from Apple is vulnerable in the same way as demonstrated last year on iPhone 5S, allowing an individual to bypass verification with a fake fingerprint created from regular glue. The technology is currently used to authenticate the owner of the device during the unlock process, as well as for approving purchases in Apple's digital stores. After cloning a fingerprint used to lock iPhone 5S and 6 devices, security researcher Marc Rogers from Lookout successfully unlocked both phones (check the video below), albeit he noticed some improvements in the latest model. He relied on the same fingerprint cloning technique used for the experiment on the 5S model last year. Rogers says that the first step is to acquire the fingerprint, which has to be clear of any smudges; a high resolution camera is also necessary for an accurate image that is then printed without any distortion, with high toner density, so that the print stick out. The next step is to impress the print on a thin layer of glue. The researcher noticed some improvements in the new sensor, as the scanning resolution is higher, experiencing greater accuracy at recognizing the real fingerprint. Moreover, during his experiment, the success with more flawed cloned fingerprints on iPhone 6 was smaller than on the 5S device, which points to the conclusion that the clarity of the print has to be higher in order to fool the Touch ID sensor. "To fool the iPhone 6 you need to make sure your fingerprint clone is clear, correctly proportioned, correctly positioned, and thick enough to prevent your real fingerprint coming through to confuse it," Rogers says in a blog post. Despite successfully unlocking the device with a fake fingerprint of the iPhone's owner, Rogers says that reproducing the experiment in the wild is unlikely to be a success because there are plenty of challenges that can be overcome in the lab, "but are likely to make it a little bit harder for a criminal to just 'lift your fingerprint' from the phone's glossy surface and unlock the device." "The attack requires skill, patience, and a really good copy of someone's fingerprint — any old smudge won't work. Furthermore, the process to turn that print into a usable copy is sufficiently complex that it's highly unlikely to be a threat for anything other than a targeted attack by a sophisticated individual," he adds. To read more click **HERE**