THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

20 August 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

August 15, Computerworld – (National) **Grocery stores in multiple states hit by data breach.** Supervalu Inc. reported that payment card data from customers at 180 of its grocery stores in several States between June 22 and July 17 may have been compromised after the company experienced a breach of its systems. Supervalu operates or provides IT services to several grocery store brands including Hornbacher's Shop 'n Save, Farm Fresh, Albertsons, ACME, Jewel-Osco, Cub Foods, and other brands. Source: http://www.computerworld.com/s/article/9250402/Grocery_stores_in_multiple_states_hit_by_data_breach

August 18, Securityweek – (International) **Windows security update causing system crash.** Microsoft removed the download links to a Windows security update and is investigating after several users reported their systems crashing upon startup after applying the update. The "blue screen of death" (BSoD) issue was found to be incorrect handling of the Windows font cache file in specific circumstances, according to a Sophos researcher. Source: http://www.securityweek.com/windows-security-update-causing-system-crash

August 18, Softpedia – (International) **New TorrentLocker ransomware uses CryptoLocker and CryptoWall components.** Researchers with iSIGHT Partners identified a new piece of ransomware known as TorrentLocker that uses elements of the CryptoLocker and CryptoWall ransomware to encrypt victims' files and demand a ransom. The ransomware is spread by spam emails and uses the Rijndael encryption algorithm. Source: http://news.softpedia.com/news/New-TorrentLocker-Ransomware-Uses-CryptoLocker-and-CryptoWall-Components-455390.shtml

August 18, Help Net Security – (International) **Gyroscopes on Android devices can be used to eavesdrop on users' conversations.** Researchers published a paper showing how the gyroscope sensors in Android devices can be combined with a speech recognition algorithm to eavesdrop on conversations due to Android gyroscopes using a sampling rate that is within a range of human voice frequency. The researchers stated that the initial results did not present a significant eavesdropping threat currently, but that it could become a vulnerability with further refinements in the speech recognition algorithm. Source: http://www.net-security.org/secworld.php?id=17266

August 17, Securityweek – (International) **Average peak size of DDoS attacks spiked in Q2: Verisign.** Verisign released its second quarter (Q2) 2014 distributed denial of service (DDoS) attack report, which found that the size of DDoS attacks increased by 216 percent compared to the first quarter of the year and that 65 percent of attacks exceeded 1 Gbps, among other findings. The report stated that the entertainment and media industry was the most attacked during Q2, followed by IT services. Source: http://www.securityweek.com/average-peak-size-ddos-attacks-spiked-q2-verisign

August 18, CNN; WREG 3 Memphis – (International) **Tennessee-based hospital network hacked, 4.5 million records stolen.** Community Health Systems, which operates 206 hospitals in 28 States, announced August 18 that the personal information, including Social Security numbers, of 4.5 million patients was stolen in April and June by China-based hackers who used sophisticated malware. The company cleared their computer systems of the malware and implemented protections against future breaches. Source: http://wreg.com/2014/08/18/tennessee-based-hospital-network-hacked-4-5-million-records-stolen/

August 18, Threatpost – (International) **New attack binds malware in parallel to software downloads.** Researchers at Ruhr University developed a proof-of-concept attack that can inject malicious code into a legitimate download that runs parallel to the original and does not modify the code, taking advantage of security deficiencies present in some free and open source software. An attacker using the attack would need to control an intermediate network node between the client and the download server, such as compromising a router, using a network redirection attack, or compromising an insider through social engineering. Source: http://threatpost.com/new-attack-binds-malware-in-parallel-to-software-downloads

August 18, Securityweek – (International) **Four-year old flaw exploited by Stuxnet still targeted.** Kaspersky Lab researchers found that vulnerability CVE-2010-2568 leveraged in the Stuxnet attacks was still present on many systems 4 years after it was patched, with tens of millions of exploits targeting the vulnerability observed between November 2013 and June 2014. The researchers also found that other older vulnerabilities are still frequently targeted, and that around 53 percent of 15.06 million detected exploits targeted Java vulnerabilities. Source: http://www.securityweek.com/four-year-old-flaw-exploited-stuxnet-still-targeted

HSBC Bank Customers Targeted by Phishing
Softpedia, 20 Aug 2014: Phishing campaigns are never taking a break and in one of their latest attempts cybercriminals seek to grab the log in credentials of the HSBC Bank customers. Crooks started spreading out emails with text designed to lure unsuspecting victims to access a website purporting to be from the bank, prompting them to log into their banking account. However, the entire website is a fake, impersonating the legitimate one from HSBC Bank. One clue showing the true colors of the scam is the connection type, which sends the information from the client to the server in an insecure manner. MillerSmiles analyzed a sample of the fraudulent email and determined the location of the fake website to be in Tehran, Iran. The incentive for accessing the link and landing in the malicious location is a message asking the potential victim to verify their account by signing in. In most cases the reason is most often a security check, in order to eliminate suspicions, but in campaign the email subject claims that the banking account is inactive. "We've noticed that your account has been inactive for some days. To safeguard your account, we've classified it as dormant," read the first lines of the message body. Phishing websites are generally alive for just a few hours but even with this short lifespan crooks still manage to make plenty of victims; moreover, they set up new domains to continue the nefarious activity. To read more click **HERE**

Community Health Systems Breach Possible due to Heartbleed Vulnerability
Softpedia, 20 Aug 2014: The breaking into the network of Community Health Systems (CHS) that ended with details of 4.5 million patients being exfiltrated by the hackers, was possible by exploiting the Heartbleed vulnerability present on a CHS Juniper device. By leveraging the flaw in the OpenSSL cryptographic library, the attackers were able to extract user credentials from the memory of the server, which were used for connecting to the systems via a VPN (virtual private network). TrustedSec, a company offering penetration testing and risk assessment services, says they obtained details about how the breach occurred and that the information about Heartbleed being at fault came from a trusted source close to the CHS investigation. As per the regulatory filling to the SEC (Securities and Exchange Commission), the initial breach of the CHS network took place in April, 2014. News of the code error in the OpenSSL library allowing the improper input validation and extracting information from the memory of the affected system, was reported by Neel Mehta of Google's security team on April 1, but it was publicly

revealed a week later. Considering the novelty of the security flaw, very few systems received a patch as soon as news of the vulnerability spread on the Internet. Also, due to its open-source nature, the OpenSSL library is so widespread that it is integrated in most things providing secure communication, from web servers, operating systems and applications to hardware devices. According to a study from Venafi, 97 percent of the Global 2000 companies had external servers that were still vulnerable to a Heartbleed attack, months after a patch was released. In the case of the CHS breach, after the perpetrators found their way into the network, reaching the 4.5 million records database was easy pickings. "This is no surprise as when given internal access to any computer network, it is virtually a 100% success rate at breaking into systems and furthering access," say TrustedSec security experts in a blog post. The operators behind the intrusion are believed to be an Advanced Persistent Threat (APT) group based in China, according to Mandiant, the forensics company that investigated the incident. On April 11, Juniper had already released updates for its SSL VPN versions 7 and 8, but applying them fell into the hands of the customers. "The time between 0-day (the day heartbleed was released) and patch day (when Juniper issued its patch) is the most critical time for an organization where monitoring and detection become essential elements of it security program," say TrustedSec experts. TrustedSec has been founded by David Kennedy, a former NSA employee, who served as Chief Security Officer (CSO) for Diebold, an ATM making company. To read more click **HERE**

"Remember Me" Feature Leaves Backdoor Open for Cybercriminals

Softpedia, 20 Aug 2014: Enabling the "remember me" or "keep me signed in" option for online accounts could pose a security risk to users, as it may be leveraged by cybercriminals to reach sensitive information. In a recent study conducted by Intercede, a company providing identity and credential management software, it was discovered that the convenient feature of staying logged into an online account for quick connection to the service could serve as a backdoor entry for threat actors. The research, carried on 2,000 consumers, showed that 75% of the subjects using social media applications and email were logged in at all times on their mobile device. Although this has a high degree of convenience when using the services, it also puts sensitive information at risk if the mobile device falls into the wrong hands. "Keeping your Facebook, Gmail, shopping and financial accounts automatically logged in might be convenient for consumers, but it's leaving the back door wide open to hackers," says Intercede's Richard Parris. The research revealed that 37% of those using Amazon and other shopping sites had the automatic login feature enabled. With mobile banking services, 23% of them resorted to the same practice, while in the case of PayPal the figure was 27%. Parris says that even if consumers are more careful with the login state in the case of the online banking services, crooks do not need access to the bank account to steal the user's identity. An email address is generally a sufficient starting point for gathering more information about the target; but the cybercriminals' efforts are decreased if they gain access to the email account, as they can work their way to compromising other accounts. The study also found that oftentimes consumers shared PIN codes and passwords with friends and colleagues. A total of 28% of the individuals questioned for the research admitted to knowing the login for mobile devices of family members, friends, and even colleagues at work. The risk for identity and data theft is increased by the fact that many of the consumers are automatically signed into accounts on multiple devices. Parris calls for a change in the way users log into their accounts, stronger authentication, and more sophisticated forms of identity being part of the solution. "As we live more and more of our lives online, all our various digital identities need to be effectively protected – worryingly, it appears that this is not the case at the moment," he says. To read more click **HERE**

Facebook Server Leveraged for DDoS Attack

Softpedia, 20 Aug 2014: The way in which images attached to Facebook posts are refreshed can be abused to conduct distributed denial-of-service (DDoS) attacks using the site's high-bandwidth servers, a security researcher found. After Facebook added a new feature for refreshing attachment content in early June, Teofil Cojocariu, security researcher at Cyber Security Research Center in Romania (CCSIR), discovered a vulnerability that permits an attacker to perpetrate a DDoS attack through the feature. He

reported the flaw to Facebook, who came up with a fix, but Cojocariu says that although larger companies are now safe from this type of attack, smaller ones with limited bandwidth resources are still susceptible to it. The fix from Facebook consists in making the unique identifier temporary, which permits a smaller number of refreshes. However, there is no information on the exact number of refreshes allowed. The researcher says that an attacker could bring down a website by using a link to an image it hosts and publishing it on Facebook with Only Me privacy parameter. By refreshing the attachment, and grabbing the browser requests, the perpetrator could create a script that would force Facebook's servers to request the file repeatedly from the source, generating a lot of traffic. Cojocariu also created a proof-of concept (PoC) script that demonstrates the attack. He says that during his tests with the PoC script the maximum bandwidth was 934.06 Mbps, but it may have been limited by the hardware used on the targeted server, which had a 1 Gbps port. He believes that there is no actual limitation on output. A similar glitch was reported to Facebook back in April, by security researcher Chaman Thapa (also known under the online handle "chr13"), but at that time Facebook said that there was no real way to create a fix "that would stop "attacks" against small consumer grade sites without also significantly degrading the overall functionality." It appears that part of the problem still remains, even after the company delivered a fix for the issue reported by the Romanian security researcher. Cojocariu discovered the vulnerability and disclosed it privately to Facebook on June 13. A day later an egineer from the company contacted him replying that the issue had been forwarded to the appropriate team. On July 28, Facebook sent Cojocariu an email informing that a fix had been implemented on the server. Cojocariu received a $500 bug bounty award for his finding. To read more click **HERE**

Users Still Getting BSODs on Windows 7 despite Microsoft's Workarounds

Softpedia, 20 Aug 2014: As you have most likely heard by now, some of the patches released by Microsoft as part of this month's Update Tuesday cycle caused more harm than good and broke down a number of Windows 7 PCs, leading to BSODs that occurred at every first boot. Microsoft was quick to confirm the issues and told us in a statement that a fix was under development, but until now no other specifics have been provided. What's worse, the workarounds that Microsoft provided don't seem to make any difference in some cases, and a number of users whose computers were impacted by the BSOD say that following the steps that are supposed to correct the problems has basically no result and leaves the errors untouched. "I'm having the blue screen issue as well, except that for a day now my screen won't work, stays black, so I can't reset, remove the update or enter BIOS (I have an ASUS K55V series notebook). I tried everything that was suggested on the internet but nothing seems to work. Has anyone faced a problem like this?" one user explains on the Microsoft Community forums. And unexpectedly, frustration among users is growing, and some of them are complaining that Microsoft doesn't care enough about its consumers to correct these problems fast. Of course, a number of posts pointed to Google and Apple as two important names that wouldn't roll out botched updates which could cause so many problems to users. "These kinds of issues make me nervous and I don't believe Microsoft takes them seriously enough... There should be a more official response and tools to help people deal with these issues," another affected user wrote. "An overly verbose Security bulletin where 90% of it is not applicable to any one individual is a pathetic communication medium.. So are user communities. I'm willing to bet Apple or Google wouldn't publish such bulletins. It needs to be as easy to identify and remove the broken updates as it is to install them to begin with." As mentioned, Microsoft is already working on a fix, and the company will most likely roll it out before the next Patch Tuesday, just to make sure that issues are repaired and everyone can use their computers flawlessly. In the meantime, if you're among these users who are experiencing a BSOD, you could give a shot to this work-around and see if it makes any difference on your computer. Just create a backup (if you can get into Windows in the first place) before everything else in order to make sure that you're on the safe side. To read more click **HERE**

OpenJDK 7 Vulnerabilities Closed in Ubuntu 14.04 LTS

Softpedia, 20 Aug 2014: Canonical has announced that quite a few OpenJDK 7 vulnerabilities have been found and corrected in its Ubuntu 14.04 LTS (Trusty Tahr) operating system. The developers have just pushed a new update for a number of OpenJDK 7 problems, fixing some security issues. "Several vulnerabilities were discovered in the OpenJDK JRE related to information disclosure, data integrity and availability. An attacker could exploit these to cause a denial of service or expose sensitive data over the network," reads the security notice. Also, "A vulnerability was discovered in the OpenJDK JRE related to availability. An attacker could exploit this to cause a denial of service." These are just a couple of the vulnerabilities identified by the developer, and for a more detailed description of the problems, you can see Canonical's security notification. Users have been advised to upgrade their systems as soon as possible. The flaws can be fixed if you upgrade your system to the latest openjdk-7-related packages specific to each distribution. To apply the patch, you will have to run the Update Manager application. In general, a standard system update will make all the necessary changes. Surprisingly enough, you won't have to restart the PC or laptop in order to apply the patch, but you will have to restart any Java apps. To read more click **HERE**

Traffic Lights System Hacked in Michigan

Softpedia, 20 Aug 2014: Basic security issues in the networked system regulating traffic flow in Michigan allowed a team of researchers to take control of about 100 traffic lights. The experiment was conducted by a team led by J. Alex Halderman, computer scientist at the University of Michigan, with the approval of a local road agency. They managed to intercept the communication between traffic sensors and controllers that communicate wirelessly, gaining complete control of the stoplights regulating the flow of vehicles on the road. In many cities across the United States the traffic flow is managed through intelligent wireless systems that rely on sensors buried below roadways to detect the cars. They send the data to a controller, which changes the traffic light. According to a paper researchers presented at the Usenix security conference in San Diego this week, in some cases, the controllers are part of an interconnected system and may communicate via radio frequency. Halderman and his team found that the controllers could be set up remotely, via an FTP connection to a configuration database. However, accessing them this way barely benefits from any protection at all. "An FTP connection to the device allows access to a writable con?guration database. This requires a username and password, but they are ?xed to default values which are published online by the manufacturer. It is not possible for a user to modify the FTP username or password," say the researchers in the paper. During the experiment, it was discovered that the traffic regulation system was riddled with elementary security flaws. The team found that the network could be easily accessed because encrypted communication was not available; controllers did not benefit from secure authentication and they were also vulnerable to known exploits. Apart from the stoplight management devices, an adversary could also attack sensors and the video cameras, which usually feature pan, tilt, and zoom control capabilities and send visual traffic information to the central server. The study shows that attackers can infiltrate the traffic network through the wireless infrastructure, and with no encryption in place or concealment of the SSID, it is enough to reverse engineer the proprietary communication protocol or to use the same type of radio hardware employed in the traffic system. "Due to the lack of encryptions, any radio that implements the proprietary protocol and has knowledge of the network's SSID can access the network," explains the paper. The results of such an intrusion are easy to predict. The actions supported by the controller include not just changing the lights based on an "if-then-else" logic, but also freezing them. Among the possible types of attacks include denial of service (setting all lights to red) leading to traffic congestion, which can also be achieved in a more subtle way, by manipulating the timings of an intersection, leaving the impression of a poorly managed road network. Also, attackers can control the lights as they wish, changing colors according to their needs (setting them to green for a specific route). A similar experiment, with the same dire consequences, was carried out by IOActive CTO Cessar Cerrudo, who presented his findings at DefCon hacker conference in Las Vegas earlier this month. To read more click **HERE**

MIT Professor's Personal Organizer Page Defaced

Softpedia, 19 Aug 2014: A hacker managed to change the looks of the personal agenda page used by a professor at the Massachusetts Institute of Technology (MIT), hosted on the university's servers. The page belongs to Tomas Palacio, an MIT Associate Professor of Electrical Engineering and Computer Science. No dirty messages were left on the page, as the hacker, who claims to be from India and goes by the online alias SaHoo, simply made it clear that he was the one behind the incident and posted some animation and an audio track. SaHoo, not affiliated with any hacker group, contacted us and said that there was no mischievous motivation behind the attack, just "a friendly hack" designed to show MIT that they need to secure their servers. Functionality of the online personal agenda does not seem to be disrupted as scrolling to the bottom of the page provide access to the full features of the script. Although there are no nefarious reasons behind the hack, SaHoo does not want to disclose the vulnerability, preferring to let the administrators find the glitch and fix it on their own. The affected page is running a VCalendar script for managing personal events. It features sections for viewing entries by day, week, month or year and provides search functionality as well as registration and login forms. VCalendar appears to have not received an update since 2006, which could mean that there are vulnerabilities that can be exploited. This may not be a serious incident, since the important resources, such as research documents, from MIT benefit from increased security on the university's servers. To read more click **HERE**