THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

25 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 21, Fairbanks Daily News-Miner – (Alaska) **University of Alaska internet outage caused by denial of service attack.** University of Alaska campuses in Fairbanks, Anchorage, and Juneau experienced a network outage for several hours August 20 after hackers targeted the university's servers with a distributed denial of service (DDoS) attack that came from multiple sources and consumed 490,000 of 500,000 available sessions on the university's firewall. The outage caused off-campus users to lose access to the university's Web sites and blocked Internet access for on-campus users. Source: http://www.newsminer.com/news/local_news/university-of-alaska-internet-outage-caused-by-denial-of-service/article_a44f2834-2905-11e4-939e-0017a43b2370.html

August 22, Softpedia – (International) **Credentials can be stolen in UI state inference attack.** Researchers presenting at the USENIX Security Symposium published a paper outlining a new form of attack called a user interface (UI) inference attack that can steal Android users' credentials by conducting a side-channel attack relying on a common shared-memory mechanism used by window managers. The attack uses a malicious app that does not require permissions and the researchers believe that the same vulnerability likely exists in other operating systems such as iOS, Windows, and OSX. Source: http://news.softpedia.com/news/Credentials-Can-Be-Stolen-In-UI-State-Inference-Attack-456028.shtml

August 22, Securityweek – (International) **Vulnerability found in Google Wallet, Alipay payment SDKs.** Researchers with Trend Micro identified and reported a security vulnerability in the in-app payment SDKs for Google Wallet and Alibaba Alipay in Android that can be exploited by attackers using intent-filters to display phishing messages and obtain user credentials. Alibaba and Google both released updates to their apps after being informed by the researchers May 27. Source: http://www.securityweek.com/vulnerability-found-google-wallet-alipay-payment-sdks

August 22, Softpedia – (International) **Vulnerability in Akeeba Backup for Joomla went undetected for years.** Sucuri researchers found a vulnerability in the Akeeba Backup extension for Joomla that has existed for years and could allow a skilled attacker to access backup files created with Akeeba and download them. The researchers stated that the security risk presented by the vulnerability was low due to the difficulty in exploiting it, and the newest version of Akeeba is no longer vulnerable. Source: http://news.softpedia.com/news/Vulnerability-in-Akeeba-Backup-for-Joomla-Went-Undetected-for-Years-455961.shtml

Kelihos Trojan Delivered as Tool to Attack US Government Websites
Softpedia, 25 Aug 2014: A new malicious campaign has been started against Russian nationals, promoting Kelihos Trojan as a tool for attacking websites under the administration of the US government. The cybercriminals appeal to the patriotism of Russian citizens to install the malware, deceiving them into thinking that the purpose of the operation is to retaliate against US-imposed sanctions to Russia. Researchers at Websense, a company providing solutions for protecting organizations from cyber attacks and data theft, discovered that the URL included in the malicious message actually leads to Kelihos Trojan, enslaving the computer of the wannabe cyber-warriors in a botnet controlled by crooks. Kelihos, also

known as Hlux, includes a diverse set of capabilities, such as sending spam, stealing sensitive information, thieving Bitcoin wallets, Bitcoin mining and using the affected computer for distributed denial-of-service (DDoS) attacks. It also creates a backdoor for the compromised system and can be used to download additional malware on the machine. Although Kelihos has been the object of multiple take-down operations carried out by law enforcement and private security companies, it has re-spawned, creating new botnets. According to Websense telemetry, the web pages hosting the malware have been barely accessed, and this campaign may be an attempt to rebuild the botnet. "What's different about this case is that instead of appealing to the victims' sense of curiosity, the cyber criminals appeal to patriotic sentiments [...], blatantly saying that they will run malware on the intended targets' computers, but without disclosing the true nature of the malware," say the researchers in a blog post. Websense says that their systems managed to block over 100,000 malicious emails between August 20 (deployment date) and August 21. Emails have different subject lines that appeal to the patriotic spirit of the receiver, and the crooks make no effort to disguise the link to the malicious file or the file itself, because they say in the message that an executable file is delivered. All the recipients had email addresses with the .ru top-level domain (TLD). The malware relies on the Winpcap driver to keep an eye on the web connections and to steal passwords from different protocols, the most targeted one being SMTP, probably to increase the distribution rate by using the infected computer to deliver spam, Websense says. "When run on the victims' computers, the bot contacts the Command & Control (C2) infrastructure over TCP, then sends an encrypted GET request to the C2 URLs (hosted in Russia and Ukraine)," explain the security experts. In some of the messages encountered by the security firm, the crooks also provide tips to disable the antivirus solution on the system, to allow installation of the malware. This is an out of ordinary method to deliver malware, but it may also be very efficient, preying on the citizen's willingness to participate in a retribution campaign against actors that took measures, political or otherwise, against their country. To read more click HERE

Info on 25,000 DHS Employees Exposed in Breach of Contractor Systems

Softpedia, 25 Aug 2014: The cyber attack on the systems of the US Investigation Services (USIS), a company running background checks for employees of the US Department of Homeland Security (DHS), exposed details of 25,000 US government workers, according to Reuters. The incident was reported at the beginning of the month, and it is believed that behind it there are actors supported by a foreign government; the incident "has all the markings of a state-sponsored attack," forensic investigators say. Reuters informs that the affected employees have received notifications about highly sensitive personal information being exposed as a result of the intrusion. The set of details accessed without authorization comprises social security numbers, education and criminal history, birth dates, as well as info about spouses, other relatives and friends, their names and addresses being included in the records. Although there is evidence of intrusion, the investigation could not determine if the perpetrators managed to actually exfiltrate the data from the USIS computer systems. After identifying the attack, USIS reported it to federal law enforcement, the Office of Personnel Management (OPM) and other agencies. As a result of the incident, OPM and DHS have both suspended their work with USIS on employee security background verifications. There is no need to stress the importance the accessed data has for foreign intelligence agencies. Dmitri Alperovitch, CTO at CrowdStrike, told Reuters that the spying entities could use these details "to identify individuals who might be vulnerable to extortion and recruitment." To read more click HERE

United States Targeted by Cyber Attacks Originating from China, the US, India, and Russia

Softpedia, 25 Aug 2014: Based on information collected from honeypots deployed in public cloud infrastructures across the globe, a company observed that most of the machines frequently targeting the US are located in China, the US, India, and Russia. Details from Alert Logic, a company providing Security-as-a-Service solutions in the cloud, show that in 32% of the cyber-attacks directed at the United States the computer systems used were located in China. Coming in second place was the US itself, as 21% of the machines used for the attacks were identified in its territory. However, this does not mean

that the attackers were in the US, only that they used systems in this country. According to an infographic provided by the company, which combines information gathered from April 1, 2013 through September 30, 2013, and relies on data from 2,200 Alert Logic customers, 17% of the machines involved in cyber incidents affecting US customers were from India, and only 9% were located in Russia. Alert Logic's attack map also reveals that computers in countries like Korea (6%), Romania (6%), Vietnam (4%) and Brazil (2%) have also contributed to the overall number of attacks, but in a lesser amount. In the case of Europe, most of the attacks (40%) originated from systems in Russia, followed by China and North and South America. As far as Asia is concerned, the US appears to have hosted most of the computers directing cyber-attacks against the region, with 63%. The type of malware used in all three regions, as per the data collected by Alert Logic, is Conficker-A, being identified in 91% of the cases in the US, 77% in Europe and 62% in Asia. The company informs that exploits for the Microsoft Directory Service (MS-DS), running on port 445, were the most prevalent for all three regions. However, the incidents were perpetrated through other vectors, HTTP being prominent for the US in 21% of the cases, followed by MySQL (13%). In Europe, HTTP, MySQL Server, MySQL, RPC (remote procedure call) and FTP were all used in 13% of the cases, while MS-DS accounted for 35% of the attacks. Most of the attacks in Asia leveraged MS-DS vulnerabilities, being used in 85% of the incidents, according to Alert Logic. Honeypots are decoy systems made vulnerable on purpose in order to catch information about the methods used by attackers to penetrate the system, as well as to collect details on the origin of nefarious activities. "While honeypots are not typically the target of highly sophisticated attacks, they are subject to many undefined attacks, and provide a window into the types of threats being launched against the cloud," says Alert Logic. To read more click **HERE**

MeetMe Social Network Systems Breached

Softpedia, 24 Aug 2014: Hackers managed to gain unauthorized access to the computer systems of the MeetMe social network, affecting an undisclosed number of users. The company discovered that the intrusion occurred between August 5 and 7, 2014, and that information on a number of accounts had been compromised. The incident was reported on August 15, but it was made public at the beginning of the week, after taking the necessary measures for preventing such events from happening and after notifying users about the intrusion and the risks it involved. According to the announcement from MeetMe, details such as user names, email addresses, and passwords have been exposed to individuals that have yet to be identified. The leaked passwords were not available in plain text as they were stored in an encrypted form on the affected server. "For a period of time, the hackers may have been able to access the affected MeetMe accounts, but there is no evidence that they did so and they can no longer do so," said the company in the breach report. Although passwords were stored securely, the company advised the affected users to change them in order to completely eliminate the threat of account hijacking. Also, if the countersign was used for logging into other services, updating them for those accounts is also recommended. According to the financial information provided by the company for the second quarter of 2014, the revenue increased by 13% compared to the same period last year, reaching a total of $10.7 / €8.08 million. The revenue from the mobile platform was up by 114%, compared to Q2 2013, being $5.6 / €4.228 million and representing more than half of the money flow recorded by the company. As far as the mobile user base is concerned, MeetMe reported in July that they had broken the barrier of one million mobile active users on a daily basis. "It took us seven years to reach 800,000 mobile daily active users. It took us another 19 months to reach 900,000 users, and then just six more weeks to reach one million users," said MeetMe CEO Geoff Cook. "We believe our exciting pipeline of new features will continue to make MeetMe the best app for finding new chat partners," he added. The company is clearly on an upward trend, which makes it a more appealing target for cyber attacks. This means that beefing up security must be a top priority these days. To read more click **HERE**

Backoff PoS Malware Impacts More than 1,000 Businesses

Softpedia, 24 Aug 2014: Point-of-sale (PoS) malware BackOff leveraged in the recent intrusion on UPS systems in 51 locations across the US is estimated to impact more than 1,000 businesses. Backoff is a recently discovered PoS malware, which is believed to have been employed in cyber-attacks on payment systems of various retailers since at least October 2013. The Department of Homeland Security (DHS), issued an advisory on Friday, recommending retailers to evaluate their payment systems for signs of compromise. "DHS strongly recommends actively contacting your IT team, antivirus vendor, managed service provider, and/or point of sale system vendor to assess whether your assets may be vulnerable and/or compromised," the advisory says. According to the communication, at the moment seven PoS providers/vendors have confirmed that their clients reported network intrusions that resulted in planting Backoff malware on the payment systems. "Reporting continues on additional compromised locations, involving private sector entities of all sizes, and the Secret Service currently estimates that over 1,000 U.S. businesses are affected," informs the DHS report. Backoff PoS malware relies on RAM scraping technique to steal track data from the memory of the affected system. It was first detected by researchers at Trustwave Spiderlabs and its existence was made public in an advisory from US CERT (Computer Emergency Response Team) on July 31. This is a different PoS malware family than the one in the Target breach, where it is believed that Kaptoxa (slang for "potato" in Russian), also known as BlackPOS, was used. To read more click **HERE**

263.35 Gbps of Traffic Aimed at One Sony Server during DDoS Attack

Softpedia, 24 Aug 2014: A distributed denial-of-service (DDoS) attack hit Sony servers on Sunday, and the hacker claiming responsibility for it says that one server was crippled by 263.35 Gbps of junk traffic. News broke that a hacker collective going under the name of Lizard Squad directed a large DDoS attack against Sony Online Entertainment and PlayStation Network services. However, it appears that the group's contribution to the incident was to merely take credit for the deed and bring more attention to it by tweeting a bomb scare to the flight carrying SOE's president John Smedley from Dallas to San Diego. The attack seems to be the act of a hacker known on Twitter as Fame (@FamedGod), who came back with a vengeance plan, making public the IP addresses of every member of the Lizard Squad collective. FamedGod tweeted that they pulled the DDoS by abusing NTP (Network Time Protocol) servers, which blasted 263.35Gbps of bad traffic towards one Sony server. In the second quarter of 2014, the largest DDoS recorded by Arbor Networks was of 325 Gbps. Verisign also registered values peaking at 300 Gbps for the same time frame; by comparison, 263.35 Gbps is far from being a light blast. Soon after launching the attack, users started to experience issues on the PSN service, being signed out due to an error (80710092) that signaled online connectivity problems. According to companies offering DDoS mitigation solutions, amplification attacks carried out through NTP servers have become more frequent in the second quarter of the year. In the case of the Sony incident, FamedGod appears to have leveraged vulnerable NTP servers. "OMG my NTP Lists are dead already. Gotta scan for new ones," a tweet says. A report in May regarding the number of NTP servers vulnerable to the "monlist" function abuse informed that 17,647 machines still needed to be patched; out of these, more than 2,100 were capable of an amplification of at least 700x. In a YouTube video, the hacker explains that the attack was possible because Sony did not implement sufficient security measures to its network following the 2011 incident, which resulted in the theft of personal details from about 77 million user accounts. FamedGod explains that "jailbreaks can access hidden and prohibited content now" and that the address of the attacked server could be discovered by decrypting a memory dump. "Memory dumping can reveal the hidden servers which personal and main information is stored. Simple hex converting and decryption lead to a full DDoS on playstations main server data center," it is said in the video. A good example to follow is Microsoft's Xbox network, which does not operate on a single datacenter. The Twitter feed of the hacker also contains a post saying that Sony could task a team with monitoring servers and filtering the bad traffic from a DDoS attack, but they would not spend the money on this. To read more click **HERE**

China to launch home-grown OS in October as Windows replacement

Computerworld, 24 Aug 2014: China hopes to launch a home-grown operating system by October to wean the country from foreign-made OSes like Windows, the government-run Xinhua news agency said Sunday. The operating system, which Xinhua did not name, will be initially offered on desktop PCs, with the plan to later extend it to smartphones. The news service cited a report in the People's Post and Telecommunications News, a trade paper run by the Ministry of Industry and Information Technology (MIIT), the agency responsible for, among other things, the regulation and development of China's software industry. "We hope to launch a Chinese-made desktop operating system by October supporting app stores," Ni Guangnan of the Chinese Academy of Engineering, told the trade paper, according to a translation by Reuters on Sunday. Ni leads an official operating system development alliance established in March by the People's Republic of China (PRC). According to the People's Post and Telecommunications News, Ni cited the end of Windows XP support and the ban on Windows 8 on government computers as giving domestic OS developers an opening. Earlier this year, China officials banned the use of Windows 8 on government computers, a move triggered by the end of Windows XP's support in April. Before that, authorities had blasted Microsoft for halting security updates to the 13-year-old OS Historically, China has been a stronghold of Windows XP, in large part because of massive piracy of Microsoft's software. China has long been at odds with foreign technology firms, particularly Microsoft and Google -- but also at times with Apple -- over their impact and influence in the country. But that animus increased significantly last month when government antitrust regulators raided several Microsoft offices, seizing computers and documents in a first step of an investigation. The probe had been prompted by complaints lodged since July 2013 about how Windows and Microsoft Office are bundled, about Windows-Office compatibility and about other unnamed concerns. The People's Post and Telecommunications News' story (Chinese language version) cited by Xinhua ran on Thursday, and provided more detail about the domestic OS plans. Ni spelled out a timeline that could replace foreign operating systems on the desktop in one to two years, then in three to five years expand to mobile devices. Private industry, Ni added, may co-fund development of the home-grown OS. "Creating an environment that allows us to compete with Google, Apple and Microsoft, that is our key to success," Ni said. China has worked on its own OS before: In 2000, Red Flag Linux, which was funded in part by the government's Ministry of Information, was released. Later that year, Red Flag was mandated as the replacement for Windows 2000 on all government PCs. Tensions at the time between China's government and Microsoft were at the root of that order. Red Flag never took off, and the company backing it shuttered earlier this year. But Red Flag -- the OS, not the company -- will be resurrected. To read more click **HERE**