THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

12 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 11, Newark Star-Ledger – (New Jersey) **Jersey City Medical Center patient data is lost on disk.** The Jersey City Medical Center notified an unknown number of Medicaid patients that their personal information, including Social Security numbers, was on an unencrypted computer disk that was lost in June. The hospital is investigating and reported that the disk was sent in a package through the United Parcel Service from the hospital to an outside company and failed to arrive at its destination. Source: http://www.nj.com/healthfit/index.ssf/2014/08/jersey_city_medical_center_loses_patient_data.html

August 11, Help Net Security – (International) **Critical 0-days found in CPE WAN Management Protocol.** Check Point researchers reported finding several zero-day vulnerabilities in CPE WAN Management Protocol (CWMP/TR-069) deployments used by major Internet service providers (ISPs) to control home and business Internet equipment which could allow large-scale malware infections able to compromise privacy, steal information, or cause service disruptions. Check Point reported the vulnerabilities to ISPs and assisted in closing them before reporting their findings publicly. Source: http://www.net-security.org/secworld.php?id=17237

August 11, Help Net Security – (International) **Smart Nest thermostat easily turned into spying device.** An independent researcher and two researchers from the University of Central Florida presenting at the 2014 Black Hat conference demonstrated how Nest smart thermostats can be compromised quickly using a USB flash drive, potentially allowing attackers to obtain information on a victim's habits as well as network information such as WiFi credentials. Compromised thermostats could also be used to connect to the Internet and be used in a variety of malicious tasks. Source: http://www.net-security.org/secworld.php?id=17239

August 9, Softpedia – (International) **10,000 impacted by resurging Facebook color changing app scam.** Researchers at Cheetah Mobile reported that a resurgence of a scam that purports to change the color scheme of Facebook has affected 10,000 users recently. The campaign steals users' Access Tokens and then attempts to install a malicious fake antivirus program or video player. Source: http://news.softpedia.com/news/10-000-Impacted-by-Resurging-Facebook-Color-Changing-App-Scam-454306.shtml

August 8, The Register – (International) **Oracle Database 12c's data redaction security smashed live on stage.** A researcher with Datacomm TSS presenting at the Defcon 22 conference demonstrated how a remote attacker could inject SQL queries to access redacted information in Oracle Database 12c due to several coding flaws. Source: http://www.theregister.co.uk/2014/08/08/oracle_database_12c_redaction_is_totally_borked_by_bad_code/

August 8, Crain's Chicago Business – (Illinois) **Chicago Yacht Club hacked.** The Chicago Yacht Club notified its members July 31 that a computer firm confirmed that malware was installed between April 26 and May 22 onto a server that hosts the club's membership database, allowing hackers to access members' personal information, including name, address, and payment card information. Source: http://www.chicagobusiness.com/article/20140808/BLOGS03/140809804

Data breaches and high-risk vulnerabilities continue to dominate
Heise Security, 12 Aug 2014: Cyber threats, data breaches and high-risk vulnerabilities have continued to dominate the first half of 2014. The severity of these attacks intensified against financial and banking institutions as well as retail outlets, according to Trend Micro. Total attacks have exposed more than 10 million personal records as of July 2014 and strongly indicate the need for organizations to adopt a more strategic approach to safeguarding digital information. These incident attacks in the second quarter affecting consumer's personal information included theft of data such as customer names, passwords, email addresses, home addresses, phone numbers, and dates of birth. These types of personal privacy breaches have affected organization's sales and earnings while leaving customers unable to access accounts and dealing with service disruption. As a result many countries have begun developing stricter privacy and data collection policies to begin dealing with this problem. As of July 15, 2014, more than 400 data breach incidents have been reported, creating the need for organizations to identify and understand their core data in order to protect and build an effective defense strategy to keep them secure. A change in mindset, organizations initially need to determine which information they regard as "core data" before devising a plan on how to protect it. Highlights of the report include:

- Critical vulnerabilities created havoc among information security professionals and the public: High-risk vulnerabilities affected various components of Internet browsing and Web services, including server-side libraries, OSs, mobile apps and browsers.

- Escalation in the severity & volume of attacks: The severity of attacks against organizations highlighted the importance of incident response planning and organization-wide security awareness.

- Cybercriminals counter online banking and mobile platform developments: Deployment of mobile ransomware and two-factor authentication-breaking malware has emerged in response to technological developments in the online banking and mobile platforms.

- Digital Life and Internet of Everything (IOE) improved way of life with emerging vulnerabilities: The 2014 FIFA World Cup held in Brazil was one of the most popular sporting events in recent history. As such, users faced various threats related to the event—one of the most widely used social engineering hooks this quarter.

- Global law enforcement partnerships lead to arrests: By sharing research findings with law enforcement agencies, financial loss prevention from cybercrime has proven effective.

To read more click HERE

How fast can security pros detect a breach?
Heise Security, 12 Aug 2014: Tripwire announced the results of a survey of 215 attendees at the Black Hat USA 2014 security conference in Las Vegas. Industry research shows most breaches go undiscovered for weeks, months or even longer. Despite this evidence, 51 percent of respondents said their organization could detect a data breach on critical systems in 24 to 48 hours, 18 percent said it would take three days and 11 percent said within a week. According to the Mandiant 2014 Threat Report, the average time required to detect breaches is 229 days. The report also states that the number of firms that detected their own breaches dropped from 37 percent in 2012 to 33 percent in 2013. "I think the survey respondents are either fooling themselves or are naively optimistic," said Dwayne Melancon, CTO for Tripwire. "A majority of the respondents said they could detect a breach in less than a week, but historical data says it is likely to be months before they notice." When asked to name the top challenges in detecting data breaches quickly, 34 percent of respondents identified too much data, specifically too many alerts and false positives, and incomplete visibility across their network and endpoints as key limiting

factors. Melancon continued: "The problem is not just 'too much data' as the survey indicates – the bigger issue is that most organizations are ignoring the foundational security controls needed to run a secure infrastructure. To read more click HERE

Millions of Computers Have Backdoor Enabled by Default

SoftPedia, 12 Aug 2014: Most computer devices come with an anti-theft solution called Computrace enabled by default, capable to execute arbitrary code with local system privileges, which does not encrypt communication with a remote server. In a presentation at Black Hat security conference in Las Vegas last week, Kaspersky security experts Vitaly Kamluk and Sergey Belov, along with Anibal Sacco from Cubica Labs, demonstrated how legitimate software Computrace, which is part of the BIOS firmware, can be used as "an advanced removal-resistant BIOS-based backdoor." The software, developed by Absolute Software and embedded in BIOS PCI Options ROM and UEFI firmware, has remote code execution capabilities by design and its purpose is to offer computer owners the possibility of remote management of the devices. However, because it does not encrypt communication with the server, it can be hijacked, if an attacker gains control over the network traffic (man-in-the-middle attack) of the affected computer. Computrace runs through two agents identified as "rpcnetp.exe" (Small Agent) and "rpcnet.exe" (Main Agent), and as Kaspersky researchers have discovered, on some systems it is enabled by default, making the machine susceptible to compromise. Vitaly Kamluk says that they do not believe that a malicious reason is behind the component being active without user consent. Instead, they think that manufacturers have it turned on unintentionally. But, regardless of the reason, the component presents a risk to users on whose machines it is enabled. The researchers found that two types of remote attacks can be conducted against Absolute Computrace, one directed at the Small Agent module and the other at the Main Agent. "It's important to note that Small Agent runs for a limited time starting from initial installation of the module and ending when the system is connected to the Internet and module is successfully updated," say the experts in the whitepaper detailing the flaw. In the second type of attack, the Main Agent is pushed to replace the Small Agent. At the beginning of the communication, no encryption is available for the protocol, but it seems that this is added at a later stage. However, cybercriminals are offered a window to take advantage of the non-encrypted protocol to gain control over the system. Because the software is not malicious and is developed by a trusted entity, most antivirus products have it whitelisted. The first glitch was discovered at the beginning of the year and reported Absolute Software at that time, but according to the presentation slides from the conference, had no reaction. The second remote code execution vulnerability, reported on June 25, generated a response from the company, who denied its existence. Computrace presence is revealed by the executables of the two agents in the list of processes as well as by connection to certain hosts. Disabling it, however, is more difficult because it is a vendor specific process, and the developer of the BIOS setup utility decides whether to include the possibility to turn on or off the Computrace module. To read more click HERE

Adobe Flash Player 14.0.0.179 Released for Download

SoftPedia, 12 Aug 2014: Adobe a few months ago decided to match its security update cycle with Microsoft's, so the company releases patches for its products every second Tuesday of each month. As a result, Adobe has rolled out today an update for Flash Player, thus fixing a number of security issues it found in the app and trying to keep users on the safe side when loading Flash content online. The official release notes are not yet available right now, as the updated build has been published on Adobe's server only a few minutes ago, but more information will most likely be provided in the coming hours. As you probably know, Microsoft will also include this Flash Player version in its Patch Tuesday rollout, as the software giant decided to patch Internet Explorer via its built-in Windows Update system. This way, Internet Explorer users do not have to manually download the new Flash Player build, as the same version will be delivered to their computer later today with the other Patch Tuesday fixes. To read more click HERE

About 23 Million of Twitter's Active Users Are Bots

SoftPedia, 12 Aug 2014: Twitter is growing steadily, but that doesn't mean that all its users are genuine. All online services face this problem, but it seems that Twitter has managed to put a number on this problem, indicating that about 23 million accounts aren't actually human. According to a new set of disclosed numbers from an SEC filing, Twitter has revealed that it has detected a lot of bot accounts, making up for some 8.5 percent of all active user accounts at the end of June. The number is quite high and investors are likely quite disappointed, especially since the company's stats aren't all that great. "We have reviewed and refined our processes, however, to calculate a new metric that is comprised of only such active users who have used applications with the capability to automatically contact our servers for regular updates where there was no discernable user action involved. In the three months ended June 30, 2014, approximately 11% of all active users solely used third-party applications to access Twitter," Twitter's note reads. "However, only up to approximately 8.5% of all active users used third party applications that may have automatically contacted our servers for regular updates without any discernible additional user-initiated action. The calculations of MAUs presented in this Quarterly Report on Form 10-Q may be affected as a result of automated activity," the company reveals. Twitter has 271 monthly active users from nearly every country of the world. The company believes that the current total audience that views content on the platform, not including syndicated content, is about two to three times the number of the actual monthly active users. To read more click HERE

Australian Users Lost over Two Million Logins to CyberVor Gang

SoftPedia, 12 Aug 2014: The CyberVor cybercrime gang is believed to hold login details of at least 2,285,295 Australian users visiting .au websites. Alex Holden, CEO of Hold Security, the company having announced last week that a specific cybercriminal Russian group had created a database with 1.2 billion unique credentials, said that the cache of information on Australian individuals contained emails and passwords. Talking to The Register, Holden also said that this data was collected from at least 5,929 ".com.au" online locations. However, this number is likely to be higher since ".net.au" domains were not included. The list of credentials could be extracted because the websites were vulnerable to SQL injection exploitation. Hold Security is currently involved in alerting the websites identified as vulnerable of the glitch, so administrators can eliminate the flaw and ensure the security of their visitors. Users are advised to change their passwords, at least for the most important online services, in order to prevent unauthorized access to their accounts. As was the case in the initial announcement, Holden did not reveal names of any of the affected websites, a decision that attracted a flurry of articles accusing that the information had been released in the context of Black Hat security conference so that the company could promote its services. The cybercriminal group believed to have what has been dubbed as "the largest cache of stolen data," has been named CyberVor by Hold Security, "vor" being the equivalent of "thief" in English. The company, which monitors underground websites for collecting information on the latest breaches and trends adopted by the crooks, says that the actual number of records in CyberVor's possession is 4.5 billion, but only 1.2 billion are unique credentials, being attached to more than 500 million email addresses. Not all the information has been stolen leveraging SQL injection vulnerabilities, as the gang first started by purchasing user information from fellow criminals. Then, they used it to attack online services that gathered large crowds of users. Later on, CyberVor relied on botnets scanning for websites vulnerable to SQL injection exploitation and reporting back to them. It appears that this operation affected over 400,000 websites. FTP locations were also targeted by the crooks, increasing the number to more than 420,000. At the moment, it is difficult to determine whether the Australians affected by the theft have been targeted in attacks such as spam and phishing, trying to lure them to websites serving malware. To read more click HERE

10,000 Records Encrypted By Synolocker at Chinese University's Faculty of Medicine

SoftPedia, 12 Aug 2014: Synolocker crypto-malware affecting Synology network access (NAS) devices in particular, has hit the Faculty of Medicine of Chinese University and took hostage no less than 10,000 patient records. It appears that the affected data belongs to the Centre for Liver Health and Institute of Digestive Disease at the Prince of Wales Hospital in Sha Tin, and the police confirmed that the crooks used Synolocker for the deed. Just like in other cases, the ransom fee for receiving the private key that can decrypt the data is 0.6 Bitcoin ($350 / €260). According to South China Morning Post, there is no evidence that the data has transpired from the storage devices, so there is no apparent risk of exposure. As soon as the infection was discovered on the affected systems, they were immediately taken offline to avoid propagation of the threat. At the moment there is no information on how the department plans to recover the files, or if a backup copy of the data exists, which would makes it possible to restore it. Attacks leveraging Synolocker ransomware have started more than a week ago, when the members of the Synology forum reported that their systems could no longer be accessed, receiving instead a ransom message asking them to pay for releasing their data. Some methods to partially rescue the files as they are encrypted have been found to be efficient, but users are advised to take precautions such as changing the connection port, disabling SSH and Telnet services and strengthening the log in password in order to reduce and even eliminate the risk of infection. To read more click HERE

Russian Point-of-Sale Hacker Pleads Not Guilty in US Court

SoftPedia, 12 Aug 2014: The Russian national that allegedly ran several carding forums and hacked into the compromised point-of-sale (PoS) systems of multiple retailers appeared for arraignment in US federal court and pleaded "not guilty" in front of the accusations. Roman Valerevich Seleznev was indicted by a federal grand jury in Washington back in 2011, but the US Secret Service managed to arrest him only this year, in Maldives, in an operation seen as controversial by Moscow. Then he was taken to Guam Island, where a court ruled that the case should be taken to the court in Washington, where Seleznev was charged. The defendant entered pleas of "not guilty" to the charges in the indictment, which include a total of 29 counts. If found guilty on all counts, he has to spend at least 65 years in prison and pay a total fine of $2,75 million / €2 million. Also known under the online aliases of "Track2," "nCuX," "Bulba," "smaus," and "shmak," Seleznev is accused of conducting cybercriminal activity between October 2009 and February 2011. As per the allegations in the indictment, he hacked into the PoS systems of various retailers and stole credit and debit card information, which he sold on carding forums he operated. The forums operated just like a regular business, where customers could buy, sell, or trade any of the goods resulted from cybercriminal activities. 30-year-old Seleznev seems to be the son of Valery Seleznev, a State Duma member representing the Liberal Democratic Party. Because of this and the tensions between Russia and the United States, the matter soon escalated, with the Russian Foreign Ministry labeling the arrest in Maldive as kidnapping, condemning the authorities for permitting such an act on its territory, to special service agents of another country. The minister also said that the United States was not at the first such act, reminding of other two Russian citizens, Viktor Bout and Konstantin Yaroshenko, convicted for attempted drug smuggling and conspiracy, brought by force into the United States. About the alleged criminal activity of Seleznev, Assistant Attorney General Caldwell said that "cyber-criminals have caused enormous financial damage and innumerable invasions of Americans' privacy, often from halfway around the world." "The alleged crimes in this case harmed thousands of U.S. citizens, and thanks to our law enforcement partners throughout the world, we will have the opportunity to seek justice in a U.S. courtroom," he added in a statement from the Department of Justice. The date of the trial has been set for October 6, 2014. To read more click HERE

Yahoo Ad Network Used to Spread CryptoWall Ransomware

SoftPedia, 11 Aug 2014: The Yahoo advertisement network has been selected by cybercriminals to carry out a malvertising type of attack on unsuspecting users, by steering them to malicious pages serving a strain of CryptoWall ransomware. When the users click on an advertisement that is connected to the crook's server, they are directed to a web page that delivers malicious files, compromising the computer.

Chris Larsen, security researcher at Blue Coat Systems, says that at a first look, the malvertising campaign did not seem like much, but it soon turned into a significant malicious operation when the nefarious ads entered the flow of major advertisement networks, such as ads.yahoo.com. “The interconnected nature of ad servers and the ease with which would-be-attackers can build trust to deliver malicious ads points to a broken security model that leaves users exposed to the types of ransomware and other malware that can steal personal, financial and credential information,” he said in a communication. According to Blue Coat’s research, the malware delivered through this campaign is CryptoWall, a program similar to the infamous CrytpoLocker. As soon as the system is infected, CryptoWall starts encrypting important data on it and holds it hostage for ransom. Unless a backup is available, and it is not affected by the encrypting capabilities of the malware, users can avoid paying the ransom. The company has identified websites that referred clients to the malicious pages in countries like India, Myanmar, Indonesia and France. Apart from these, Blue Coat says that adsmail.us has also been used to refer unsuspecting users to the threat delivering online locations. Major advertising networks are always sought by cybercriminals to deliver their malware because of their broad potential to reach a large amount of users. Among other types of threats that have been inserted in legitimate advertising wasMagnitude Exploit Kit; it is worth noting that Yahoo has no fault with this, because their service was included in the advertising trail created by smaller service providers, likely in cahoots with the crooks. Yahoo offers a diverse range of services, to both individuals and businesses, and as such, bad actors always try to introduce their malicious code so that it gets delivered to an extraordinarily wide audience. In recent Yahoo-related reports, the service’s Twitter account for delivering news (@YahooNews), has been hacked for a brief time on Sunday, and the perpetrator managed to smuggle in the feed a message saying that there was an Ebola outbreak in Atlanta. Control over the account was soon regained, as 18 minutes later the owners informed of unauthorized access and advised followers to disregard the tweet. To read more click HERE