THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

6 August 2014

August 5, IDG News Service – (International) **Oracle issues fix for Java update that crippled some Web apps.** Oracle issued an update for Java 7, Java 7 Update 67, which contains a fix for an issue in the recent Java 7 Update 65 that caused some Web applications to be unable to launch. Source: http://www.computerworld.com/s/article/9250163/Oracle_issues_fix_for_Java_update_that_crippled_some_Web_apps

August 5, The Register – (International) **Multi function p0wnage just getting worse, researcher finds.** A researcher with Rapid 7 reported that multi-function printers from several companies contain vulnerabilities that can allow an attacker to access usernames, email addresses, and passwords from corporate Active Directory accounts. The researcher and his team reported being able to gain access to corporate networks in 40-50 percent of attempts. Source: http://www.theregister.co.uk/2014/08/05/printer_pwnage_just_getting_worse_researcher_finds/

August 5, Help Net Security – (International) **DDoS attack volumes plummet as NTP servers got patched.** Black Lotus released its Q2 2014 Threat Report which found that patching weaknesses in systems decreased distributed reflection denial of service (DrDoS) attacks by 86 percent in the second quarter of 2014 while multi-vector attacks such as TCP SYN and HTTP GET attacks increased 140 percent during the quarter, among other findings. Source: http://www.net-security.org/secworld.php?id=17206

August 5, Securityweek – (International) **Mobile users targeted with SandroRat posing as security software.** Researchers with McAfee identified a campaign targeting Android users in Europe which disguises the SandroRat malware as a Kaspersky mobile security app to trick users into installing it. The malware is spread via text messages and emails and purports to be from a bank as a means of enhancing mobile security. Source: http://www.securityweek.com/mobile-users-targeted-sandrorat-posing-security-software

August 5, Securityweek – (International) **Flaw enabled access to internal Yahoo administration panel.** A researcher with RMSEC identified and reported an issue with Yahoo that allowed him to guess a correct URL and then be logged into an internal content management system (CMS) with full administrator rights. Yahoo closed the issue after being informed by the researcher. Source: http://www.securityweek.com/flaw-enabled-access-internal-yahoo-administration-panel

August 5, Securityweek – (International) **Apache Cordova vulnerabilities expose Android apps.** IBM Security Systems researchers identified three vulnerabilities in the Apache Cordova developer APIs that could allow attackers to steal sensitive information from applications created using Apache Cordova. The Apache Cordova development team was notified by the researchers prior to public disclosure and an update was released August 4 that closes the flaws. Source: http://www.securityweek.com/apache-cordova-vulnerabilities-expose-android-apps

August 4, Threatpost – (International) **RAT malware communicating via Yahoo Mail.** A researcher with G-Data published an analysis of a remote access trojan (RAT) known as IcoScript that has mostly gone undetected since 2012 and uses Yahoo Mail to communicate with its controllers to avoid creating suspicious traffic. The RAT could also be modified to use Gmail or other webmail providers. Source: http://threatpost.com/rat-malware-communicating-via-yahoo-mail

Email Scam Uses Legitimate Sender Address

SoftPedia, 6 Aug 2014: Emails coming from legitimate users, known to the victim, have been spotted to deliver messages asking for money that would get the alleged friend out of some sort of trouble. Cybercriminals started to hijack email accounts and use them to perpetrate this type of scam. In one of the messages seen by Christopher Boyd from Malwarebytes, the sender pretended to be in a bit of a jam in a foreign country and required some money in order to settle hotel bills and catch a flight home. Because the potential victim sees that the sender is a friend, the scam's rate of success is likely to increase, especially with a well-crafted text. In the sample presented by Boyd, the crook got hold of the email account of the recipient's landlord and asked for financial aid to get back home, from Istanbul. The fictitious reason was that some robbers took all their money and mobile phones, leaving the passport, though. With no money in the pocket, the landlord has to pay for the hotel. Despite contacting the embassy, it appears that settling the hotel bill is all that stands between the landlord and the flight back home. The security researcher says that the email address of the landlord had been compromised and used for spreading the deceitful message to all contacts available. "This tactic has been around for years, and is often found on social networks where close connections add a sense of trust and 'oh no, my poor friend' to the proceedings," he said. Such scams are generally easy to spot, especially when the message comes from someone close, whose whereabouts are known to the recipient. Scammers do not spend time analyzing communication, and in most cases, they recycle text from other campaigns, setting off the alarm bells of a potential victim. All users have a particular way to write messages when using a digital form of communication, and spotting a change is not too much of an effort. Also, since text is recycled from one campaign to another, searching it on Google before deciding to reply is always a good idea. "Checking with mutual contacts to see if they received the same message is often suggested as evidence of fake messages, but keep in mind that someone desperate for help with no phone access could well decide to send a message to as many of their contacts as possible," writes the security researcher. He also suggests establishing a specific word that should be used in emergencies when communicating via email or mobile text; this way the recipient will be sure about the legitimacy of the message. To read more click **HERE**

Magnitude Exploit Kit Is a Well-Oiled Crimeware

SoftPedia, 5 Aug 2014: Security researchers took a close look at the Magnitude Exploit Kit (EK), a malicious package accounting for a large portion of the exploit kit market share and famous for being used to infect high-profile websites such as Yahoo Ad Network and PHP.net. Trustwave managed to learn about the inner workings of the threat after examining its administration panel, which revealed a well-oiled crime machine ready to adapt in order to evade attempts from security companies to disrupt its activity. The control page of the package offered its operators complete information on the infection rates, domain blacklisting, antivirus detection rates for the exploits, self-imposed geo-IP restrictions preventing malware spread, and details about the victims's machine (operating system and web browser used) and country. Moreover, Trustwave reports that Magnitude's administration panel also provides the latest news about the EK. For instance, the operators posted that they made the decision to reset statistics twice a week, for security reasons. At one point, they let other users know that the malware delivery mechanism had been improved and that the infection rate should see an increase. Magnitude EK relied on just three exploits, one for Internet Explorer 6 through 10, responsible for most infections (85%), and the other two for Java. Trustwave researchers found that the EK delivered no less than seven malware pieces to the victim, allowing its customers to use their own malicious files. For a better understanding of the efficiency of this exploit kit, it should be said that out of 1.1 million attempts of infection, 210,000 machines fell victim.

This amounts to a 20% rate of success in a single month, with multiple different threats delivered to the victims's computers. The operators behind Magnitude did not discriminate and targeted absolutely any machine that could be infected. Trustwave says that "a few hundred of the machines that Magnitude attempted to infect were from government agencies from the US, Canada, UK and several other countries. Also recorded computers from several universities in Australia, Hong Kong, the US and others." At the top of the list of countries most affected by Magnitude EK are United States, France, Iran, and the UK. In just a few weeks, a total of 211 unique malware samples were distributed by the package and each successful compromise meant that the victim's computer received five or six of them, sometimes belonging to the same malware family. Magnitude Exploit Kit was used to deliver all sort of malware, from info stealers (Alureon, Tepfer, Zeus) to crypto-malware (CryptoWall) and backdoors (Nymaim, Vawtrak, Simda). Multiple security solutions on the market offer protection against it at the moment. To read more click **HERE**

Military Cyber Warriors Crushed by Civilian Hackers in Supersecret Cyber War Game

SoftPedia, 5 Aug 2014: In a secret cyber war game, whose details and final results remain confidential, hackers from the military service were totally crushed by opponents from the civilian sector. One Capitol Hill staffer that attended the exercise, which took place in a secret compound at Fort Meade, Maryland, said that the active-duty team was "pretty much obliterated," and that they "didn't even know how they'd been attacked." US Cyber Command (CYBERCOM) started operating in 2010 and is currently training about 6,000 soldiers for protecting the Department of Defense networks from intrusions, as well as for running offensive operations to disable enemy systems. The civilian sector team was composed of IT security specialists who face real-world threats. It seems that the experience of real scenarios is far more valuable, as hackers have to deal with actual advanced threats that need to be squashed. "The guys and gals who work day jobs in suits and ties — or tie dyes and blue jeans — a lot of them have real-world experience in cyber that is far and above the limited skills that ... regular military people have," Navy Times quoted Matthew Aid, a technology and intelligence expert. Initially, CYBERCOM drew a plan mixing 80% active-duty personnel and 20% civilians. Arnold Punaro, chairman of the Reserve Forces Policy Board (RFPB), said that "it defies common sense to think that industry, in particular our high-tech industries, are not moving at light speed compared to the way government works," and the results of the cyber war game confirmed that. To read more click **HERE**

1.2 Billion Unique Credentials, 500 Million Email Addresses Stolen by Russian Cyber Gang

SoftPedia, 5 Aug 2014: After a research of more than seven months, a security company from the United States discovered that a Russian cyber gang managed to collect 1.2 billion unique credentials from more than 420,000 websites and FTP locations. The cybercriminals were indiscriminate as far as the breached sites were concerned, targeting websites of both small businesses and larger ones. Discovered by Hold Security firm in Milwaukee, the total amount of stolen records is 4.5 billion, and apart from credentials consisting of names and passwords, the database also contains more than 500 million email addresses, linked to those credentials. The company named the gang currently holding all this information CyberVor, "vor" standing for "thief" in Russian. Acquiring the data, which is the largest known collection in history, could be achieved through the simplest and common (although quite efficient as CyberVor demonstrated) form of attack: SQL injection. However, the operation was conducted at a large scale from the beginning. After getting some databases with stolen credentials from other hackers on the black market, CyberVor gang used them "to attack e-mail providers, social media, and other websites to distribute spam to victims and install malicious redirections on legitimate systems," explains a post from the company. The group changed their method at the beginning of the year and got access to information from different botnets that were basically scanning the Internet for websites with SQL vulnerabilities. According to Hold Security, the infected machines would check for SQL weak spots on every site they accessed. It is believed that the infected systems "conducted possibly the largest security audit ever. Over 400,000 sites were identified to be potentially vulnerable to SQL injection flaws alone." Even if the numbers appear mind-blowing at first glance, there is a good chance that the amount of valid information amassed by the

cybercriminals is lower. One reason for this is that, with so many online services requesting registration of an account, there are plenty of users that rely on a disposable email address in the process. Hold Security advises companies to check their websites for SQL injection vulnerabilities, since there is a great possibility that most of them are still susceptible to exploitation. The Milwaukee-based security firm is not new on the scene of uncovering big data leaks. They were the ones that identified a breach on Adobe Systems in October 2013, in which source code (40GB of encrypted archives) from their flagship products became available on servers of known hackers. They also identified and tracked the incident at Target that caused data on 40 million credit and debit cards to be leaked along with guest information on another 70 million individuals. To read more click **HERE**

Microsoft Signals the Death of Service Packs with Monthly Windows Updates

SoftPedia, 5 Aug 2014: We have already known that Microsoft isn't planning to roll out any new service packs for Windows, but this time the company has publicly suggested that it's giving up on this strategy for future Windows versions. In a blog post announcing this month's update rollout for Windows 8.1, which has also been used to kill off rumors pointing to a possible Windows 8.1 Update 2, Microsoft explains that it's no longer willing to wait several months to deliver a large pack of improvements for its operating systems. Instead, the company says, users will be offered monthly updates that are included in the Patch Tuesday rollouts and provide a number of enhancements, not necessarily concerning the security of the operating system. Microsoft explains that sometime, these monthly updates could also bring new features, although nothing exciting is expected to be released until Windows 9 officially gets to see daylight. "Rather than waiting for months and bundling together a bunch of improvements into a larger update as we did for the Windows 8.1 Update, customers can expect that we'll use our already existing monthly update process to deliver more frequent improvements along with the security updates normally provided as part of 'Update Tuesday.' So despite rumors and speculation, we are not planning to deliver a Windows 8.1 Update 2," Microsoft explained in a statement yesterday. All Windows improvements will obviously be shipped through Windows Update, as is the case with the Patch Tuesday fixes released every single month. This way, Windows users could get it with little effort, making everything a seamless process that's appropriate for both beginners and those more experienced. "We'll continue to use our normal channels such as Windows Update (WU), Microsoft Update (MU), and Windows Server Update Services (WSUS) to deliver updates to Windows. These updates will include security updates to help keep you protected, as well as non-security updates that can bring a range of improvements to your PC or tablet running Windows," the company says. Windows 7 thus remains the last operating system which received a service pack per se, although some say that Windows 8.1 and Windows 8.1 Update could easily be considered service packs as well for the core Windows 8 operating system. Microsoft however has switched to a faster release cadence, and waiting for service packs that could be released every 12 months isn't quite the best option, so expect even more things to change with the release of Windows 9. To read more click **HERE**

Target Provides Update on Expenses Related to the 2013 Data Breach

SoftPedia, 5 Aug 2014: Relying on currently available information, Target has updated the estimates for the expenses related to the breach of its systems discovered in December 2013, which resulted in data loss affecting up to 110 million customers. A statement from the company informs that the forecast cost relating to the breach is $148 million, out of which $38 is covered by insurance. "Expenses for the quarter include an increase to the accrual for estimated probable losses for what the Company believes to be the vast majority of actual and potential breach-related claims, including claims by payment card networks," reads the statement. Target says that the estimates rely on proper evaluation, with current information, historical precedents and assessment of the validity of claims being contributing factors to the conclusion. However, the company is aware of the fact that the numbers may change as new information is revealed, leading to potential material losses beyond the current forecast. On the other hand, determining such possible losses cannot be calculated at the moment. "The accrual does not reflect future breach-related

legal, consulting or administrative fees, which are expensed as incurred and not expected to be material in any individual period," the statement also added. To read more click HERE

About 72,500 TotalBank Customers Notified of Personal Data Exposure

SoftPedia, 5 Aug 2014: TotalBank officials have learned of a security breach on their system that may have led to the exposure of customer information relating to personal or business accounts to unauthorized individuals. The incident was discovered on June 24 this year, and measures to initiate an investigation were taken immediately, outside data forensics experts being hired for the evaluation. The personal information exposed to the intruders consists of names, addresses, account numbers, account balance, and personal identification number (for example, social security number, driver's license number, passport number, and alien registration number). In a notification to the affected customers, which are reportedly about 72,500, the bank said that the leaked details did not include login credentials that could permit an intruder to access their bank accounts. "We want to assure you that we have reinforced our internal security protections and firewalls, enhanced threat detection and monitoring, and shut down access to any compromised system. We are also continuing to work closely with law enforcement." "As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you," informs the notification. Besides the identity protection solutions provided by the institution, bank officials advise users to keep a vigilant watch on suspicious or unauthorized activity. To read more click HERE

Here's How Gmail Detected the Child Abuse Photos inside Gmail

SoftPedia 5 Aug 2014: Google helped with the arrest of a man who, as you may have heard, was sending indecent images of children to a friend. The news made the world have contradictory feelings about Google's email scanning activities because, on the one hand, it's great that the man was captured, but on the other hand, there's a big question about everyone's privacy level while using Gmail. Google has come out and said that they are only scanning emails for advertising, and child abuse footage is the only type of content they flag while scanning. This means that other type of criminal activities remain under the radar or, at least, they're not reported by Google to the authorities. Even so, the company's assurances haven't really made people relax about the whole situation because it's long been feared that Google oversteps its boundaries when it scans emails, which is also considered a controversial practice. The company has even been sued for its email scanning habits, but since April, everything has been put in the Terms of Service to make sure that Google is no longer liable in any court for scanning emails for advertising purposes. So, how does Google detect indecent pictures but leaves everything else alone? Well, the company has been working with authorities, such as the National Center for Missing and Exploited Children, for many years. In the time that has passed since then, the Internet giant has built a database full of hashes, also known as photo fingerprints, for various child abuse images. Each one is unique and they're attached to a certain image, so it doesn't matter if someone changes the name of the file. When Google scans the email and its contents while the messages is being sent, received and stored to the cloud, as per the company's ToS, the system also detects these hashes. The company is then legally obligated to report them to the authorities, who can then obtain warrants and eventually arrest the culprits. The company is adamant about keeping its powers restricted to fighting against child abuse and has been working to take down any links from its search results that may lead to such sites, as well as actual images from the search engine, not just Gmail. Other companies have similar systems in place. Microsoft, for instance, has PhotoDNA, a piece of software that can be used to detect images of abuse. Similarly, this one too can calculate a mathematical hash for images of child sexual abuse, which immediately recognizes photos even if they were altered in one way or another. Both Facebook and Twitter use this technology. Therefore, you shouldn't worry about Google alerting the cops if you share family photos with your kids with some close family and friends. To read more click HERE