THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

1 July 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

June 30, Securityweek – (International) **Energy companies in Europe, US hit by sophisticated attack campaign.** Symantec researchers identified an ongoing cyberattack campaign by a group known as Dragonfly or Energetic Bear targeting the energy sector in the U.S. and several other countries. The campaign has used phishing emails, watering hole attacks, and a recently-uncovered compromise of several industrial control system manufacturers' Web sites. Source: http://www.securityweek.com/energy-companies-europe-us-hit-sophisticated-attack-campaign

June 30, Securityweek – (International) **"Emotet" banking malware steals data via network sniffing.** Researchers at Trend Micro identified a new piece of banking malware dubbed Emotet that attempts to steal banking credentials by logging outgoing traffic and comparing it against a list of targeted financial institutions. The malware is distributed via spam emails containing a link to a malicious Web site, and currently is primarily targeting financial institutions in Germany. Source: http://www.securityweek.com/emotet-banking-malware-steals-data-network-sniffing

June 27, Al.com – (Alabama) **Tuscaloosa Police arrest former hospital employee for stealing data from DCH Regional Medical Center.** The Tuscaloosa Police Department arrested a former employee June 26 in connection to stealing data from a clearing house used by DCH Regional Medical Center after files were removed June 16. The medical center is investigating and will notify any patients affected by the data download. Source: http://www.al.com/news/tuscaloosa/index.ssf/2014/06/tuscaloosa_police_arrest_hospi.html

June 30, WXIN 59 Indianapolis – (Indiana; California) **Butler alumni, current and prospective students warned of data breach.** Butler University in Indianapolis informed 163,000 current and past students and employees that their personal and financial information may have been compromised in a hacking incident sometime between November 2013 and May. The university began its investigation after authorities in California arrested an individual in possession of a flash drive containing information of Butler University employees. Source: http://fox59.com/2014/06/30/butler-university-alumni-current-students-warned-of-data-breach

June 30, The Register – (International) **London teen charged over Spamhaus mega-DDoS attacks.** Authorities in the U.K. charged a teenager for his alleged involvement in several major distributed denial of service (DDoS) attacks against anti-spam service Spamhaus during 2013. The attacks were also led to worldwide disruptions in Internet exchanges and services. Source: http://www.theregister.co.uk/2014/06/30/ddos_charges/

June 30, Threatpost – (International) **PHP fixes OpenSSL flaws in new releases.** The PHP Group released new versions of PHP, closing two vulnerabilities in OpenSSL that are related to timestamps. Source: http://threatpost.com/php-fixes-openssl-flaws-in-new-releases/106908

June 30, Help Net Security – (International) **Google Drive update fixes data-leaking flaw.** Google closed a security issue in its Google Drive service that previously allowed some files shared with a direct link to be accessed by unauthorized third parties. Some files could still be seen by unauthorized parties, and Google advised users with files that met certain criteria to remove them. Source: http://www.net-security.org/secworld.php?id=17067

Email Security Notifications from Microsoft Are Back On
SoftPedia, 1 Jul 2014: Microsoft has decided that the service of providing security notifications to professionals via email should not be interrupted and announced that it would resume on Thursday, July 3. Last week, Microsoft informed IT professionals who signed up to receive notices of security updates that starting July 1 they would no longer be delivered the messages containing advanced notifications related to security. The information in these emails gives system administrators a heads-up about the upcoming changes generated by the Windows update cycle, and it also delivers various security advisories. The decision to stop the service was caused by a new Canadian spam law that goes into effect on July 1. However, said law did have exceptions that exempted Microsoft's service. Subscribers to the security emails were advised to use the security feeds of the company in order to stay informed. However, Microsoft had a change of heart and issued a statement that brings things back to normal and re-instates the service. "On June 27, 2014, Microsoft notified customers that we were suspending Microsoft Security Notifications due to changing governmental policies concerning the issuance of automated electronic messaging. We have reviewed our processes and will resume these security notifications with our monthly Advanced Notification Service (ANS) on July 3, 2014," it reads. To read more click **HERE**

Microsoft Word Macro Attack Aims at Rich Targets
SoftPedia, 1 Jul 2014: A very well-conceived spear-phishing campaign using Office Macro attack vector has been discovered to target victims in banking, oil, television, and jewelry industries. Researchers at Cisco have analyzed how the new threat operates and have noted that the cybercriminals take advantage of the Visual Basic Scripting for Applications feature in Microsoft Word to deliver the malware to the victim's computer. "When the victim opens the Word document, an On-Open macro fires, which results in downloading an executable and launching it on the victim's machine," the Cisco blog post says. Using macros in malicious campaigns is an old approach, but in this case, the threat actors have combined the cloud storage services from Dropbox to host the payloads. Luring the victim to open the document is done through an email that purports to be an invoice, purchase order or receipt created specifically for the target. Should the victim launch the attached Word file, the malicious executable is retrieved from Dropbox by the macro and once on the computer, it contacts several domains. The cloud storage account hosts a total number of four pieces of payload for the exploit; Dropbox has been notified by the Cisco researchers and the share links have been disabled. Upon investigating the domains contacted by the malicious file, which are believed to be command and control servers, the security researchers found clues in the whois records that allowed them to link the group behind this operation to a number of other domains and email addresses. Furthermore, the information helped trace other malicious campaigns, relying on other pieces of malware that could be associated with this particular threat actor. Cisco researchers said that the amount of information uncovered by digging into the whois records and examining matching details with other domains and campaigns is quite vast and it also led to associating some of the contact addresses to domains using privacy protection services. Evasion attempts were also recorded, as whois records would change between browser refreshes. "If you monitor whois history you can still view all of this information, including the evasion attempt. While we were performing the investigation, items like addresses, email addresses, and such were changed, literally, in between browser

refreshes." The starting point for the researchers was the "londonpaerl.co.uk" domain, a typo-squat of the "londonpearl.co.uk," which is a reputable supplier of cultured pearls and jewelry. From the analysis of the domain's whois records and passive DNS information, it appears that these cybercriminals have been in the business since at least 2007. To read more click **HERE**

Houston Astros' Systems Breached, Trade Talks Revealed

SoftPedia, 1 Jul 2014: The systems of the Houston Astros baseball team have been accessed by an unauthorized person, who extracted content revealing internal trade talks. The details regarding the method used by the perpetrator to gain access to confidential data is not known, but a weak password might be involved. The Houston Astros created an online database, called "Ground Control," a few years ago, specifically designed for private use. It allows communication with other front offices and it also offers player statistics and video. At the moment, there is no official information, except for the confirmation of the incident, but Deadspin speculates that the intrusion was due to weak password protection. All the documents stolen from the database have been made public on Anonbin.com, an online repository similar to Pastebin, where documents can be posted anonymously. Multiple executives confirm authenticity of trade talks hacked from Astros computer. Despite the leaked details, Astros GM Jeff Luhnow commented on the incident before the game against Seattle Mariners on Monday and said that "not all the information that was published was accurate. Some it was not. I really can't get into what's accurate and what wasn't. But we're going to pursue it and try to find out who did it and prosecute them." He also said that the FBI is involved in the case and that the perpetrator is going to be prosecuted. To read more click **HERE**

What's New in iOS 7.1.2 – Specific Fixes, Security

SoftPedia, 1 Jul 2014: Apple is now offering iOS 7.1.2 both over-the-air (OTA) and through iTunes, while the security side of the update has also been disclosed in a standard advisory. See what's new in this release as we prepare for the massive iOS 8 rollout this fall. iOS 7.1.2 was handed to end users yesterday evening around 19:30 (GMT+2), at which point there was little information about the update. Some users wouldn't even receive the OTA notification until several hours later, and the security document that listed many of the patches included in the update was hidden from sight. Not anymore. We now have the full scoop on Apple's intentions with iOS 7.1.2, including the numerous security fixes that occurred in this release. "This update contains bug fixes and security updates," Apple says. One of the patches improves iBeacon connectivity and stability, and there are also some code corrections for data transfer for 3rd-party accessories, including bar code scanners. An issue with data protection class of Mail attachments is also patched, but this is just scratching the surface as far as iOS 7.1.2 is concerned. An advisory titled "About the security content of iOS 7.1.2" reveals that the update packs dozens of patches for recently found flaws in WebKit, Certificate Trust Policy, Kernel, CoreGraphics, launchd, Lockdown, Lock Screen, and many other areas. Some of the most serious vulnerabilities deal with Activation Lock. "Devices were performing incomplete checks during device activation, which made it possible for malicious individuals to partially bypass Activation Lock. This issue was addressed through additional client-side verification of data received from activation servers," Apple explains. Another such flaw would allow someone with physical access to the iDevice to exceed the maximum number of failed passcode attempts. The fruity company explains that "In some circumstances, the failed passcode attempt limit was not enforced. This issue was addressed through additional enforcement of this limit." A vulnerability that was widely discussed by security researchers last month, "Data protection was not enabled for mail attachments, allowing them to be read by an attacker with physical access to the device," reads the description of a Mail flaw. "This issue was addressed by changing the encryption class of mail attachments," Apple says. Available via iTunes or OTA, iOS 7.1.2 is compatible with iPhone 4, iPhone 4S, iPhone 5, iPhone 5s, iPhone 5c, iPad second generation, iPad third generation, iPad fourth generation, iPad Air, iPad mini, iPad mini with Retina display, and iPod touch fifth generation. Read through Apple's full advisory to see what else has been fixed in terms of security. Since it includes so many patches, the update is highly recommended

to everyone running iOS 7. Also worth noting is that the Pangu jailbreak still works with this new firmware, according to reports. To read more click HERE

Apple Releases Safari 7.0.5 and Safari 6.1.5 with Security Fixes

SoftPedia, 1 Jul 2014: In tandem with OS X 10.9.4 and Security Update 2014-003, Apple today offers Safari 7.0.5 for Mavericks and Safari 6.1.5 for Lion and Mountain Lion customers, featuring patches for newly-found security issues. Addressing more than a dozen separate WebKit flaws in the browser, Apple is offering two distinct updates, one for OS X Mavericks users, the other specifically tailored to OS X Lion and Mountain Lion. The vulnerabilities discovered in WebKit are identical across all three OS X versions. For example, multiple corruption issues in the page rendering engine affected OS X Lion v10.7.5, OS X Lion Server v10.7.5, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.3. "Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution," Apple says. The issues have been addressed through improved memory handling, according to the advisory. Another flaw could lead to the disclosure of local file content by dragging a URL from a maliciously crafted website to another window. "This issue was addressed through improved validation of dragged resources," according to the Mac maker. Yet another WebKit vulnerability would allow a maliciously crafted website to spoof its domain name in the address bar. Apple improved encoding of URLs, thus patching the flaw. Safari 7.0.5 is included in the Mavericks 10.9.4 update, whereas Safari 6.1.5 must be downloaded separately by users of OS X Lion and OS X Mountain Lion. These are likely the last updates Safari will get before Apple releases the all-new version of the browser in OS X Yosemite this fall. In Yosemite, Safari gets a streamlined toolbar that displays your most important controls front and center, while at the same time giving you more room to view actual content. Users will further get new ways to access their favorite sites, have more control over privacy matters, and manage their tabs with ease. An improved Nitro JavaScript engine will facilitate blazing-fast browsing, while the latest web standards are also implemented (such as WebGL). You can open a window in Private Browsing mode and surf the web without having your browsing history saved, while other windows can remain in regular browsing mode. Also in Yosemite, you can search the web directly in Spotlight and Safari will automatically summon suggestions from sources like Wikipedia, Bing, Maps, news, and iTunes, as well as results from the search engine you selected as default. To use Safari 7.0.5 and Safari 6.1.5, your Mac needs at least OS X Lion (version 10.7). To read more click HERE

After Windows 8, China Bans Microsoft Office

SoftPedia, 1 Jul 2014: China has made another important step in moving away from Microsoft software by banning the Office productivity suite, only one month after the country decided to make Windows 8 a forbidden product on government computers. A report published today by CRI reveals that the central government has asked a number of departments to stop using Microsoft Office and instead go for locally-developed productivity suits, such as the one belonging to Kingsoft, which also tries to compete with Redmond in this particular market. While no clear details have been provided, it's pretty obvious that Microsoft is losing ground in China, which remains one of the largest markets across the world. Even though piracy levels in China are still high, Microsoft clearly sees the local market as a big opportunity, so the company continues negotiations with local authorities to make sure that its products, including Windows 8 and Office, get a chance to be installed on government computers. The company told us in a statement last month that while Windows 8 is indeed forbidden on government computers, Windows 7 is still available, so it's offering this particular OS version as a replacement until all discussions come to a conclusion. "We were surprised to learn about the reference to Windows 8 in this notice," the company said in a mailed statement. "Microsoft has been working proactively with the Central Government Procurement Center and other government agencies through the evaluation process to ensure that our products and services meet all government procurement requirements. We have been and will continue to provide Windows 7 to government customers. At the same time we are working on the Window 8 evaluation with relevant government agencies." People close to the matter previously hinted that the Windows 8 ban is mostly China's very own payback after the software giant pulled the plug on Windows

XP. China has only recently moved government computers to genuine copies of Windows XP, so country officials considered that Microsoft should at least provide extended support in order to keep them protected after such a difficult upgrade process. Microsoft obviously refused to do so and explained that China, just like any other country out there, needs to upgrade computers to Windows 7 or Windows 8.1 and, if they really want extended support, they should pay for it. The Chinese officials responded by blocking Windows 8 in the country and pushing local departments to an open-source alternative that would gradually replace all Windows installations. To read more click **HERE**

British Teen Charged with Computer Misuse

SoftPedia, 1 Jul 2014: A 17-year-old from London has been charged with several offenses, computer misuse and fraud being among them, as a result of an investigation conducted by the National Crime Agency in the United Kingdom. According to a statement from the law enforcement agency, the teen was arrested last year in April, after multiple distributed denial-of-service (DDoS) attacks that resulted in the disruption of Internet exchanges and services all over the world. Upon arresting him, the police officers seized a number of electronic devices. The detectives from the National Crime Agency also found that the suspect had "a significant amount of money flowing through his bank account." There isn't much information available in the statement, but judging by the fact that last year's major DDoS incident that fits the details above was against Spamhaus, one could conclude that the 17-year-old was part of the group that conducted it. Up until February this year, when an almost 400Gbps DDoS attack was mitigated, the one against Spamhaus held the record for the largest amount of junk traffic directed towards a target. Online reports from September of last year tell of an arrest back in April which "followed an international police operation against those suspected of carrying out a cyber attack so large that it slowed down the internet." We contacted the National Crime Agency for more details on the matter, but we have not received a reply yet. To read more click **HERE**

A Lighter ZeuS Is Discovered

SoftPedia, 1 Jul 2014: A new variant of the infamous ZeuS Trojan has been discovered to host a more limited set of functions than the original. The differences are noteworthy and can still have a significant impact. Malware authors do not waste time, even after a major takedown has forced them to relinquish access to the command and control servers for the infected machines. The new version, uncovered by Fortinet last week and named ZeuS Lite, relies only on TCP to communicate to the remote server and has the initial server list encrypted and hardcoded in the malware body, together with the packet cipher key. Encryption of the network data is no longer carried out with the RC4 algorithm, as the authors implemented the more secure AES-128. However, it appears that the authors have implemented a second layer of encryption for incoming and outgoing communication, a simple byte-to-byte XOR algorithm, which is used at first. Then, the data is encoded once more using AES-128. Another difference when compared to the original is the support for control over the infected machine, as the malware can perform commands for shutting down the system, rebooting it, executing external programs or scripts, or updating the malicious components. Kan Chen of Fortinet says that "Even though it is shorter, this new version of Zeus is capable of performing sophisticated tasks that could cause great harm to the infected host," and that the features it includes amount to increased flexibility, which allows downloading new malicious functions from the remote servers and executing them. To read more click **HERE**