The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
16 April 2014

Purpose
Educate recipients of cyber events to aid in the protection of electronically stored corporate proprietary, DoD and/or Personally Identifiable Information from theft, compromise, espionage, and / or insider threat

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, Sandia 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 open source data

April 15, Softpedia – (International) **RCE, information disclosure and XSS flaws found in PayPal Partner Program.** A security researcher identified and reported a cross-site scripting (XSS) issue and an information disclosure issue that could be leveraged for remote code execution in the PayPal Partner Program's payment processor Web site. The issues were later closed by PayPal. Source: http://news.softpedia.com/news/RCE-Information-Disclosure-and-XSS-Flaws-Found-in-PayPal-Partner-Program-Video-437634.shtml

April 15, Softpedia – (International) **Expert finds SQL injection, RCE vulnerabilities in Flickr Photo Books.** A security researcher identified and reported a SQL injection vulnerability and a remote code execution vulnerability in Flickr's Photo Books Web site that could allow an attacker to gain access to Flickr's databases. Yahoo closed the vulnerabilities after a second report by the researcher. Source: http://news.softpedia.com/news/Expert-Finds-SQL-Injection-RCE-Vulnerabilities-in-Flickr-Photo-Books-Video-437724.shtml

April 15, Help Net Security – (International) **Hardware manufacturer LaCie suffered year-long data breach.** Computer storage manufacturer LaCie stated that the FBI informed the company of a data breach where malware was used to gain access to customer transactions carried out on the company's Web site. LaCie temporarily disabled the e-commerce portion of its Web site and will be resetting users' passwords in response. Source: http://www.net-security.org/secworld.php?id=16693

April 15, Help Net Security – (International) **Heartbleed: VMware starts delivering patches.** VMware announced that it began issuing patches for its products affected by the Heartbleed OpenSSL vulnerability, with patches for all affected products expected by April 19. Source: http://www.net-security.org/secworld.php?id=16692

April 14, Softpedia – (International) **Flash SMS flaw in iOS can be exploited to make the lock screen unresponsive.** A security researcher identified a Flash SMS flaw in iOS that can be used to make a device's lock screen unresponsive, which could be used for ransom attacks. The flaw was fixed with the release of iOS 7.1 but devices running previous versions of the mobile operating system are vulnerable. Source: http://news.softpedia.com/news/Flash-SMS-Flaw-in-iOS-Can-Be-Exploited-to-Make-the-Lock-Screen-Unresponsive-437566.shtml

Java JRE 8 Update 5 Released for Download
SoftPedia, 16 Apr 2014: Java JRE 8 Update 5 was officially launched today, coming with a long list of improvements, as well as bug fixes and security enhancements for all Windows users. According to the official release notes, the new version changes the frequency of some security dialogs, so they now show up less often to make sure that users aren't bothered so much. At the same time, it also comes with some new options aimed at developers and although regular users might not be so interested in this, it's still important for everyone to update. Quote from the change log provided to us this morning: "If a stand-alone asterisk (*) is specified as the value for the Caller-Allowable-Codebase attribute, then calls from JavaScript code to RIA will

show a security warning, and users have the choice to allow the call or block the call." Plenty of bug fixes have also been included in the package, while the feature lineup remains basically unchanged, which means that you can still create apps on a single platform and use them virtually everywhere, no matter the operating system the target device is using. Overall, this new update should be great news for everyone creating apps in Java, so download Java JRE 8 Update 5 right now to see what's new. To read more click **HERE**

Canadian Police Has Suspects for Heartbleed Breach That Exposed 900 SINs
SoftPedia, 16 Apr 2014: The Canadian Police has announced that it has identified an individual that could be responsible for a Heartbleed data breach reported by the Canada Revenue Agency. According to a statement, the issue had in fact been discovered last week, which prompted the Canadian authorities to shut down several sites in order to patch up the security hole, CBC reports. During this time, the police was actually investigating the security breach that saw some 900 social insurance numbers being stolen. "This deferral permitted us to advance our investigation over the weekend, identify possible offenders and has helped mitigate further risk," the police said. Originally, only the site belonging to the Canadian Revenue Agency was taken down, but other government sites followed later in the week. On Friday, the CRA realized that a six-hour attack that exploited the Heartbleed vulnerability stole 900 social insurance numbers. However, the National Democratic Party wants to know whether the government could have done more to avoid the security breach in the first place, especially since it spent days patching the Heartbleed bug, which shouldn't have taken so long. The lengthy intervention and the fact that the sites weren't taken down earlier may have allowed the hackers to steal the information without leaving a trace. "What's really disturbing is the lack of clarity on what CRA did when they found out about the Heartbleed bug," said Charlie Angus, member of the Parliament. Their justified concern is why it took so long for the CRA to patch the bug, especially since Heartbleed was exposed on Monday, and on Friday, the agency's database was still not secure. Heartbleed affects several versions of OpenSSL, which were used to secure about two thirds of the world's websites. Attacks made by exploiting Heartbleed do not leave any traces on the affected servers, which makes it impossible to know how many times hackers used it or if there were any prior attempts. This, of course, raises the question about how exactly the authorities managed to track down one or more hackers. While many believe that Heartbleed was placed in OpenSSL on purpose, the programmer responsible for the massive security problem says that it was a simple error, with no malicious purpose. He also explained that he'd been working on OpenSSL and checking it for bugs for a long time. If the error had happened in another area, it wouldn't have been so dangerous, but due to its placement, it affected the security of billions of people. To read more click **HERE**

Hackers Are Scanning the Web for Websites Vulnerable to Heartbleed Attacks
SoftPedia, 16 Apr 2014: While many companies have already updated their OpenSSL installations to prevent cybercriminals from stealing their customers' information by exploiting the Heartbleed bug, there are a number of services that are still vulnerable. Experts at the University of Michigan have been monitoring Heartbleed attacks and vulnerable websites with the aid of ZMap, an open-source network scanner that can be used to perform Internet-wide network studies. Shortly after news of Heartbleed came to light, experts noted that they had observed a small number of hosts scanning for the vulnerability. On April 10, researchers revealed spotting attempts to exploit the Heartbleed bug by an IP address in China. The IP in question is known for being associated with malicious activities. A second attempt came from an Amazon EC2 instance. "Since our honeypot address is not a major site, we suspect that these attack attempts were part of Internet-wide exploit attempts. We didn't observe any such wide-scale attacks prior to the public announcement of the bug. However we cannot rule out that the possibility that there were earlier targeted attacks against specific sites," computer scientists at the University of Michigan wrote in their report. On Tuesday, they revealed seeing 41 unique hosts scanning for Heartbleed and attempting to exploit vulnerable systems. 59% of the hosts are located in China and they've accounted for 45% of attacks. In the meantime, Johannes Ullrich of the SANS Internet Storm Center has told AFP that while many companies have patched their websites, there's also a downside to this entire situation. The expert believes that the Heartbleed fix might slow down Web performance. The main problem is

with digital certificates. Because of the OpenSSL vulnerability, companies have to revoke old ones and obtain new private keys. While updating keys is usually not an issue for Web browser vendors, the fact that a lot of organizations are changing their certificates at the same time could prove problematic. At one point, users might be getting a lot of errors referring to invalid certificates. This could lead to people ignoring errors of disabling security checks in their browser. This could then be leveraged by cybercriminals. To make matters worse, Trend Micro reports that mobile applications are also impacted by the Heartbleed bug. Initially, the security firm said that mobile apps were affected because the servers they connected to were vulnerable. However, after a closer investigation, researchers have determined that the apps themselves are vulnerable because of a bundled OpenSSL library. To read more click **HERE**

Oracle Fixes 104 Security Holes with April 2014 CPU

SoftPedia, 16 Apr 2014: Oracle has released its Critical Patch Update (CPU) for April 2014. A total of 104 security fixes are included in the latest update, the company has announced. The list of affected products includes Database, Fusion Middleware, Access Manager, Containers for J2EE, Data Integrator, Endeca Server, Event Processing, OpenSSO, WebCenter Portal, WebLogic Server, Hyperion Common Admin, E-Business Suite, Agile PLM Framework, Transportation Management, PeopleSoft Enterprise, Java SE, MySQL Server and others. Unsurprisingly, many of the vulnerabilities impact Java SE. Of the total of 37 Java SE security holes, 35 can be remotely exploited by an attacker without the need of authentication credentials. The patches for many of the products are cumulative, which means that they include the all the fixes from previous CPUs as well. The vulnerabilities fixed with the April 2014 CPU have been reported by Andrea Micalizzi (rgod), Borked of the Google Security Team, Christopher Meyer of Ruhr-University Bochum, Ilja van Sprundel of ioactive.com, Jörg Delker, the Red Hat Security Response Team, Timo Warns, Yuki Chen of Trend Micro, and many others. Oracle advises customers to update their installations as soon as possible. The next update is scheduled for July 15, 2014. For additional details, check out the Oracle Critical Patch Update Advisory for April 2014 (**LINK**). To read more click **HERE**

ESET Says Windows XP Users Should Disconnect Their Computers from the Internet

SoftPedia, 16 Apr 2014: Windows XP is quite a trending topic these days given the fact that it no longer receives support and security patches, but that doesn't necessarily mean that users are ready to give up on it. Instead, 28 percent of the desktop computers worldwide are still running XP, which is living proof that many users are still addicted to the operating system launched nearly 13 years ago. ESET, maker of famous anti-virus product NOD32 and one of the companies whose applications will continue to work on Windows XP for at least two more years, provided some tips for those still running the unsupported operating system, saying that security software is a must-have these days on every single computer that sticks to the ancient platform. One of the recommendations made by ESET is to disconnect your system from the Internet whenever it's possible, as cybercriminals would obviously attempt to exploit their data using malware delivered via email, compromised websites, and file-sharing applications. "If the computer does not have to be connected to the Internet, disconnect or disable the connection so that the PC can only connect to other machines on the same non-Internet network. This will ensure that Internet-borne threats cannot directly attack your XP PC, and will make it harder for an attacker to steal data off the computer," ESET said in a press statement today. Of course, deploying the final updates for Windows XP and the latest versions of the software applications running on your computer is also a way to stay secure, as this could help you block any security issues that might exist in the programs you previously installed. "In addition to the operating system and drivers, you should also make sure you have the latest versions of your application software on the computer, and that those are fully-patched and updated. Users should make sure that security software should be updates with security program that combines signature-based and heuristic detection, includes a firewall, and has some kind of host intrusion protection system," ESET pointed out. Microsoft, on the other hand, says that everyone should migrate to a newer OS version as soon as possible, as third-party software cannot block all threats trying to exploit vulnerabilities found in the operating system. The company obviously wants users to move to Windows 8.1, the newest version of the OS that’s said to be the most secure and reliable edition to date. To read more click **HERE**