The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

27 May 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

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

May 22, Los Angeles Times – (California) **L.A. County finds 3,500 more patients affected by data breach.** County officials in Los Angeles reported May 22 that an additional 3,497 patients may have had their personal information stolen in a February theft of 8 computers from the Torrance office of Sutherland Healthcare Solutions, bringing the total number of patients affected to roughly 342,000. The newly identified patients were Department of Public Health patients who had received Drug Medi-Cal services, and the incident is still under investigation. Source: http://www.latimes.com/local/lanow/la-me-ln-county-data-breach-20140522-story.html

May 23, Threatpost – (International) **Apple patches 22 Safari Webkit vulnerabilities.** Apple released an update for its Safari browser May 22, patching 22 vulnerabilities in the Webkit browser engine that could be exploited in drive-by download attacks. Source: http://threatpost.com/apple-patches-22-safari-webkit-vulnerabilities

May 22, IDG News Service – (International) **Microsoft will patch IE zero day but doesn't give timeline.** Microsoft announced May 22 that it plans to patch a use-after-free vulnerability in Internet Explorer (IE) 8 disclosed by the HP Zero Day Initiative May 21. Source: http://www.networkworld.com/news/2014/052314-microsoft-will-patch-ie-zero-281863.html

May 22, Threatpost – (International) **Android Outlook app could expose emails, attachments.** Researchers at Include Security made public May 21 details of two content encryption issues in Microsoft's Outlook app for Android after first reporting the issues to Microsoft in December 2013. The issues involve the storage of email attachments on devices' SD card partitions that could make them accessible to any app or third party with physical access. Source: http://threatpost.com/android-outlook-app-could-expose-emails-attachments

May 22, The Register – (International) **Better safe than sorry: SourceForge pushes password reset.** SourceForge asked its users to change their passwords as part of an update to the site's security systems. New passwords will then be stored in a more secure manner in accordance with the updated policies. Source: http://www.theregister.co.uk/2014/05/22/better_safe_than_sorry_sourceforge_pushes_password_reset/

Hackers can digitally hijack your iPhone and hold it for ransom
Yahoo, 27 May 2014: If it wasn't our devices and data at risk, it would be pretty fascinating to see the creative new ways hackers find to attack various systems. But it is our data and devices being compromised constantly by nefarious hackers, and their latest tactics use Apple's own security tools against Apple device owners in one of the most devious hacks we have seen in quite some time. The Age on Tuesday reported news of a new scam that hackers have begun perpetrating in Australia. A number of iPhone, iPad and Mac owners in Western and Southern Australia awoke Tuesday morning to find that their devices had been locked using Apple's Find

My iPhone,Find My iPad and Find My Mac Features. These features were designed to allow users to remotely locate Apple devices that have been lost or stolen, and they also allow users to lock their lost devices and display a message to aid in their recovery. Hackers in Australia have found another use for Apple's remote locking feature, however. They have been able to compromise Apple's iCloud-based remote device locking feature in order to render iPhones, iPads and Macs useless. They then display a message on the devices that demands a ransom be paid via PayPal before they will unlock the devices. This latest news of Apple's systems being compromised comes just one week after hackers claimed they were able to hack iCloud and unlock iOS devices. Those looking to prevent this devious new attack should ensure that they have PIN code or password protection enabled on their devices. Two-factor authentication can also be used to further protect iCloud accounts. To read more click **HERE**

Multiple Linux Kernel Vulnerabilities Closed in Ubuntu 14.04 LTS

SoftPedia, 27 May 2014: A number of Linux kernel vulnerabilities discovered in the Linux kernel affecting the Ubuntu 14.04 LTS (Trusty Tahr) operating system have been fixed by Canonical. Besides all the packages that are updated during a maintenance cycle of an operating system, the Linux kernel also receives regular new versions that usually take care of vulnerabilities and other problems. This is rarely done to introduce new features, but users should upgrade nonetheless. "A flaw was discovered in the handling of network packets when mergeable buffers are disabled for virtual machines in the Linux kernel. Guest OS users may exploit this flaw to cause a denial of service (host OS crash) or possibly gain privilege on the host OS." "A flaw was discovered in the Linux kernel's ping sockets. An unprivileged local user could exploit this flaw to cause a denial of service (system crash) or possibly gain privileges via a crafted application," reads the official security notification. These are just two of the vulnerabilities closed by this update, which should arrive on the regular channels when using the Software Updater. The security flaws can be fixed if users upgrade the system(s) to the linux-image-3.13.0-27-generic, (3.13.0-27.50), but this is only true for Ubuntu 14.04 LTS (Trusty Tahr). Other operating systems feature different Linux kernels and the versions will be different. Upgrading the Linux kernel is not something to be taken lightly. Most of the time, some important fixes are implemented with new versions of the kernel and users should upgrade as soon as possible. We must also warn users who have manually installed their video drivers. It's possible that you will have to reinstall the kernel headers for the video drivers, especially if you are using NVIDIA hardware and proprietary drivers. Canonical has pledged to support the operating system until 2019, which means that, if you stick with this distribution, you might be the beneficiary of countless similar updates. Don't forget to reboot your computer after the upgrade, and be careful. Make sure you save any work you're doing before hitting that button. To read more click **HERE**

AVAST Forum Hacked, User Passwords Being Reset

SoftPedia, 27 May 2014: AVAST has once again fell victim to hackers, as the company's forum was attacked during the weekend and all user names, nicknames, email addresses and passwords were compromised. Vince Steckler, CEO AVAST Software, confirmed the attack today and announced that the company decided to take the forum offline in order to continue work on resetting all user passwords in order to keep everyone protected. Users will be asked to set new passwords when they log back in, Steckler explained, and everyone is recommended to change their passwords in case they're using it on some other websites as well. "If you use the same password and user names to log into any other sites, please change those passwords immediately. Once our forum is back online, all users will be required to set new passwords as the compromised passwords will no longer work," he said. AVAST claims that only the forum was compromised and no other details have been accessed, which means that financial details or any payment information is completely safe. "This issue only affects our community-support forum. Less than 0.2% of our 200 million users were affected. No payment, license, or financial systems or other data was compromised," Steckler continued. As far as the stolen passwords are concerned, the security vendor explained that all of them were hashed, but an experienced thief could still decrypt them and thus gain access to user accounts. That's why everyone will have to set a new password when the forums are back online. At the same time, AVAST says that it doesn't have any details right now as to how the

attackers managed to break into the forums, but added that the new version, which will be soon online, will be based on a new platform that provides enhanced stability and security. "We are now rebuilding the forum and moving it to a different software platform. When it returns, it will be faster and more secure. This forum for many years has been hosted on a third-party software platform and how the attacker breached the forum is not yet known. However, we do believe that the attack just occurred and we detected it essentially immediately," the company explained. This is basically the second very important security breach of the month, after online retailer eBay asked users to change all their passwords as soon as possible due to a similar hack. AVAST's forum is still offline at the time of writing this article, but it's expected to be brought back online in the next 24 hours. To read more click **HERE**

Don't Log In to WordPress via Open WiFi or Your Blog Could Get Hijacked

SoftPedia, 27 May 2014: If you often access your WordPress account via an open WiFi hotspot or other unsecured network, you could be exposing yourself to hijackers. Regardless of whether you've enabled two-factor authentication to your account or of how much precaution you usually take, the next person to lose control over their account could be you. This was discovered after a staff techie over at the Electronic Frontier Foundation, Yan Zhu, noticed that the WordPress servers were sending an important browser cookie in plain text, without any type of encryption layer. While this may seem like common security practice, it looks like this may have slipped through the cracks at WordPress. The cookie that Zhu refers to comes with the tag "wordpress_logged_in" and is set once a user fills in a valid WordPress user name and password. This means that the individual gains access to private messages, updates and the dashboard for the owner's blog if the cookie is stolen. If this particular cookie is transmitted without encryption, then it can easily be intercepted and hijackers can gain access to the WordPress blogs, post messages, delete content, change things however they want. The one thing that wasn't possible was to change passwords, since that is dependable on another cookie that is actually encrypted. Zhu has really managed to do all these things. She grabbed the cookie from her own account like a hacker would, pasted it into a new browser profile and went to WordPress where she wasn't even prompted to log in, despite the fact that two-factor authentication was enabled for the account. WordPress admitted to the security problem and promised an update in the near future. However, the company mentioned that the cookie could only be used until it expired. Considering that it actually remains valid for three years, that's not really a solution. As mentioned, a fix for the issue will be included in the next WordPress update. Thankfully, however, WordPress sites that are hosted individually on a server with HTTPS support are not vulnerable as long as the added security layer is enabled for each page. Either way, everyone should refrain from accessing WordPress accounts via open WiFi spots. This is a serious security vulnerability for WordPress and if someone meant to do harm, this would be easy. To read more click **HERE**

Apache Tomcat 7.0.54 Now Available for Download

SoftPedia, 27 May 2014: Apache Tomcat 7.0.54, an open source software implementation of the Java Servlet and JavaServer Pages technologies, developed under the Java Community Process, is now available for download. It's been a while since the latest Apache Tomcat release, but this only means that the devs had more time to get more fixes and changes into the software. This is a source package, so regular users don't really need it. According to the changelog, the custom UTF-8 decoder has been fixed, more options have been added for managing the FIPS mode in the AprLifecycleListener, an infinite loop has been avoided if an application calls session.invalidate() from the destroyed session, removing an MBean notification listener now reverts all the operations performed when adding an MBean notification listener, and information about finished deployment and its execution time has been added to the log files. Also, a few additional locations where, theoretically, a memory leak could occur have been patched, the authentication of users when using the JAASMemoryLoginModule has been fixed, and a regression in the handling of back-slash has been corrected. To read more click **HERE**

Cyber Thieves Took Data on 145 Million eBay Customers by Hacking 3 Corporate Employees

Reuters, 27 May 2014 EBay Inc initially believed that its customers' data was safe as forensic investigators reviewed a network security breach discovered in early May and made public this week, a senior executive told Reuters on Friday. EBay has come under fire over its handling of the cyberattack, in which hackers accessed personal data of all 145 million users, ranking it among the biggest such attacks launched on a corporation to date. "For a very long period of time we did not believe that there was any eBay customer data compromised," global marketplaces chief Devin Wenig said, in the first comments by a top eBay executive since the e-commerce company disclosed the breach on Wednesday. EBay moved "swiftly to disclose" the breach after it realized customer data was involved, he said. Wenig would not say when the company first realized that the cyberattackers accessed customer data, nor how long it took to prepare Wednesday's announcement. He said hackers got in using the credentials of three corporate employees, eventually making their way to the user database. Hackers accessed email addresses and encrypted passwords belonging to all eBay users. "Millions" of users have since reset their passwords and the company had begun notifying users, though it would take some time to complete that task, Wenig said. "You would imagine that anyone who has ever touched eBay is a large number," he said. "So we're going to send all of them an email, but sending that number all at once is not operationally possible." At least three U.S. states are investigating the company's security practices. Customers have complained on social media about delayed notification emails. And New York's attorney general called on eBay to provide free credit monitoring services to users. But the Internet retail giant has no plans to compensate customers or offer free credit monitoring for now because it had detected no financial fraud, Wenig said. Wenig declined comment when asked if he thought eBay had good security prior to the breach. He said the company would now bolster its security systems, and has mobilized senior executives in a subsequent investigation of the attack. "We want to make sure it doesn't happen again so we're going to continue to look our procedures, harden our operational environment and add levels of security where it's appropriate." Buying and selling activity on eBay remained "fairly normal" though eBay is still working out the cost of the breach, which included hiring a number of security firms. Wenig, who was previously a senior executive at Thomson Reuters Corp, declined to comment on whether the cost could be material to eBay's results. Wenig's revelation that the company initially believed that no customer data had been compromised might take some of the heat off eBay's executive team. Cyber forensics experts said it's not uncommon for large companies to take weeks to grasp the full impact of an attack, because hackers are often able to steal data without leaving obvious clues. "In some cases you go in and find the smoking gun immediately. Other times, it takes a few days or even a few weeks," said Kevin Johnson, a cyber-forensics expert who was not involved in the eBay investigation but has worked for other Fortune 500 companies. Daniel Clemens, a forensics expert and CEO of Packet Ninjas, said investigators often ask companies to hold off on disclosure until they believe they understand the full extent of an attack. Otherwise, they risk tipping off attackers who might cover their tracks or leave "back doors" so they can return after the investigators complete their probe. On Wednesday, the e-commerce company announced that hackers raided its network between late February and early March. The company said financial information was not compromised and its payments unit PayPal was not affected. When eBay first discovered the network breach in early May, the senior team was immediately involved and held multiple daily calls on the issue. EBay staff have been working around the clock since Wednesday. Wenig said he could not provide much more detail about what happened in the attack beyond the scant information given out so far. He declined to provide further specifics, citing ongoing investigations by the Federal Bureau of Investigation and several forensics firms including FireEye Inc's Mandiant division. To read more click **HERE**