The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

13 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

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

May 9, Becker's Hospital Review – (Texas) **1,981 Baylor Regional Medical Center patients' information compromised by phishing scheme.** Baylor Regional Medical Center in Plano notified 1,981 patients April 25 that their information was compromised after the medical center discovered some physicians, who had patients' personal information in their email accounts, responded to phishing emails in February. Source: http://www.beckershospitalreview.com/healthcare-information-technology/1-981-baylor-regional-medical-center-patients-information-compromised-by-phishing-scheme.html

May 12, Softpedia – (International) **Bitly says hackers breached offsite database backup.** Bitly enabled two-factor authentication for all its accounts on its hosted source code repository after learning hackers gained access to customer accounts from an offsite database backup storage, that was not initiated by the company, through a compromised employee account. Source: http://news.softpedia.com/news/Bitly-Says-Hackers-Breached-Offsite-Database-Backup-441677.shtml

May 9, The Register – (International) **Point DNS blitzed by mystery DDoS assault.** Point DNS reported a high intensity distributed denial-of-service (DDoS) attack which knocked out all of its domain name system (DNS) servers for several hours May 9. The company believes the attack originated from China and is investigating the size and techniques used. Source: http://www.theregister.co.uk/2014/05/09/point_dns_ddos/

May 9, IDG News Service – (International) **Rush to defend against Heartbleed leads to mistakes with certificates, patches.** Netcraft released a report May 9 stating 30,000 sites that revoked their compromised SSL certificates after the Heartbleed vulnerability reissued new ones with the same private keys as the old certificate and that around 57 percent of sites vulnerable have not revoked or reissued their SSL certificates. Source: http://www.networkworld.com/news/2014/050914-rush-to-defend-against-heartbleed-281465.html

Adobe Flash Player 13.0.0.214 Now Available for Download
Softpedia, 13 May 2014: Just as promised, Adobe today released an updated version of Flash Player that brings fixes for some of the security issues recently discovered on all supported platforms. Adobe has already confirmed in a security advisory released last week that it's planning to patch a number of vulnerabilities today, the same day when Microsoft is rolling out this month's Patch Tuesday improvements. In addition to Flash player, Adobe Reader and Acrobat are also getting fixes. "Adobe is planning to release security updates on Tuesday, May 13, 2014 for Adobe Reader and Acrobat XI (11.0.06) and earlier versions for Windows and Macintosh," Adobe said in a security advisory. Of course, the new release is available on all supported platforms and is considered a mandatory update for all those who have already installed one of the aforementioned affected products, no matter if they are using Windows or Mac devices. As far as Windows is concerned, XP is also part of this new update cycle, so make sure that you download Adobe Flash Player 13.0.0.214 no matter the Windows version that's powering your computer. At the same time, it also supports the newer Windows 8.1 and 8.1 Update, in both 32- and 64-bit flavors. To read more click **HERE**

Adobe Reader XI 11.0.7 Released for Download

SoftPedia, 13 May 2014: Adobe Reader XI 11.0.7 is now available for download on Windows platforms and although no release notes are available at this point, everyone is recommended to deploy the update as soon as possible. Since its Patch Tuesday and Adobe has synchronized its patching cycle with Microsoft's, the company is expected to roll out some security improvements for its software today, so it's safe to assume that Adobe Reader XI 11.0.7 comes with fixes supposed to fix vulnerabilities and other glitches that could be used by hackers to break into one's computer. Adobe Reader XI 11.0.7 continues to work flawlessly on basically all Windows versions on the market, including Windows XP, whose end of support was officially announced on April 8. This means that Windows XP no longer receives updates and security patches, so it's critical for Adobe to fix flaws in its software. The feature lineup of Adobe Reader remains unchanged, so you get the same powerful options to view PDF documents and print them easily, no matter what operating system version you're using. Overall, this update should come in handy especially for Windows XP users, so download Adobe Reader XI 11.0.7 right now to make sure that all security vulnerabilities in the application are completely fixed. To read more click **HERE**

Cybercriminals Use Microsoft Word Flaw in Attacks Targeted at Taiwanese Government

Softpedia, 13 May 2014: Back in March, Microsoft issued a warning regarding a remote code execution vulnerability in Word, that was being leveraged by cybercriminals in targeted attacks. The company patched the security hole in April, but experts have found that cybercriminals are still relying on it in their campaigns. According to Trend Micro, the Word vulnerability has been leveraged in targeted attacks against government agencies and an educational institution in Taiwan. The attack against government agencies relied on emails carrying malicious attachments. The messages purported to come from a government employee, and they contained an exploit identified by Trend Micro as TROJ_ARTIEF.ZTBD-R. This component drops additional files which ultimately lead to the final payload detected as BKDR_SIMBOT.SMC. The operation against the educational institution relied on an email discussing free-trade issues. The file attached to the emails was designed to drop a backdoor, BKDR_SIMBOT.ZTBD-PB, which enabled cybercriminals to steal sensitive files from the targeted organization. Experts believe that the attacks are part of a campaign dubbed Taidoor, which has been active since 2009. In addition to these actions, cybercriminals have also been leveraging the Word vulnerability in an attack targeting a Taiwanese mailing service. In this operation, the malicious actors rely on the PlugX RAT to steal files and take control of infected machines. For additional technical details on the attacks targeted at Taiwanese organizations, check out Trend Micro's blog (**link**). To read more click **HERE**

Microsoft Extends Windows 8.1 Update Installation Deadline

Softpedia, 13 May 2014: Microsoft today announced that Windows 8.1 users have one more month to install Windows 8.1 Update, as the company extended the installation deadline from May 13 to June 10. This means that those who are still having issues deploying Windows 8.1 Update still have enough time to cope with the issues and find a way to resolve them. Microsoft said in a blog post today that some users have indeed experienced problems when they tried to install Windows 8.1 Update, so that's why it's extended the deadline to June 10. "While we believe the majority of people have received the update, we recognize that not all have. Having our customers running their devices with the latest updates is super important to us. And we're committed to helping ensure their safety. As a result, we've decided to extend the requirement for our consumer customers to update their devices to the Windows 8.1 Update in order to receive security updates another 30 days to June 10," Microsoft's Brandon LeBlanc said. Windows 8.1 Update is being delivered via Windows Update, but a number of users have turned to the manual installation method in order to cope with some of the errors that occurred during the setup process. Microsoft already provided a number of workarounds to help users experiencing issues, but it remains to be seen if everyone manages to install the new OS version using these tweaks. To read more click **HERE**