THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

1 October 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

September 30, Softpedia – (International) **Variant of Upatre malware dropper seen in bank emails.** A security researcher reported finding a new variant of the Upatre malware dropper attached to emails purporting to be from financial institutions. The new variant is distributed as a download through a link in the malicious emails and has a low VirusTotal detection rate. Source: http://news.softpedia.com/news/Variant-of-Upatre-Malware-Dropper-Seen-In-Bank-Emails-460463.shtml

September 30, Help Net Security – (International) **Apple patches Shellshock bug in OS X.** Apple released a security update for its OS X operating system that closes two remotely exploitable vulnerabilities in the GNU Bash UNIX shell known as Shellshock. Source: http://www.net-security.org/secworld.php?id=17430

September 30, Securityweek – (International) **'Shellshock' attacks could already top 1 billion: Report.** Incapsula researchers reported that the company's Web application firewall deflected over 217,000 attempted exploitations of the Shellshock vulnerability in GNU Bash during the 4 days after the vulnerability was disclosed and estimated that the total number of attacks attempting to exploit the flaw could reach 1 billion. Source: http://www.securityweek.com/shellshock-attacks-could-already-top-1-billion-report

September 30, Softpedia – (International) **Seller of StealthGenie mobile spyware app indicted and arrested.** The CEO of InvoCode was arrested September 27 in Los Angeles for allegedly selling and advertising the StealthGenie mobile spyware. The Pakistani national allegedly worked with others to develop and market the spyware that is compatible with major mobile operating systems such as Android, Blackberry, and iOS. Source: http://news.softpedia.com/news/Seller-of-StealthGenie-Mobile-Spyware-App-Indicted-And-Arrested-460448.shtml

September 29, Softpedia – (International) **Signed CryptoWall delivered via malvertising campaign on top-ranked websites.** Researchers with Barracuda Labs identified a variant of the CryptoWall ransomware signed with a valid digital certificate from DigiCert and spread through malicious ads on the Zedo ad network to several popular Web sites. As of September 29, the CryptoWall variant was detected by 12 of 55 security solutions on VirusTotal. Source: http://news.softpedia.com/news/CryptoWall-Delivered-Via-Malvertising-Campaign-on-Top-Ranked-Websites-460375.shtml

September 29, Threatpost – (International) **RadEditor web editor vulnerable to XSS attacks.** A researcher identified and reported a cross-site scripting (XSS) vulnerability in the RadEditor text editor used in several Microsoft products that could allow attackers to inject malicious script and obtain private data. The vulnerability was closed by Telerik September 24. Source: http://threatpost.com/radeditor-web-editor-vulnerable-to-xss-attacks

September 29, Softpedia – (International) **All CloudFlare customers benefit from Universal SSL.** CloudFlare announced September 29 that it was providing all customers with SSL certificates under its Universal SSL service to enhance security. Source: http://news.softpedia.com/news/All-CloudFlare-Customers-Benefit-from-Universal-SSL-460374.shtml

September 30, Securityweek – (International) **New data breaches hit Supervalu, Albertson's.** Supervalu officials reported a second incident September 29 where hackers installed a different piece of malware on the company's computer system that potentially captured customers' payment card information from the payment processing systems of four Cub Foods stores in Minnesota and several Albertson's grocery stores across the U.S. between August and September. Source: http://www.securityweek.com/new-data-breaches-hit-supervalu-albertsons

How to avoid the horrible iOS 8 bug that could delete your files

BGR, 1 Oct 2014: Apple has had one headache after another over the past few weeks, spanning from the media circus that is "Bendgate" to a buggy iOS 8.0.1 update that bricked about 40,000 new iPhone 6 and iPhone 6 Plus handsets. Among all of these issues lies a fairly serious bug in iOS 8 that has been causing major headaches for users — but luckily, there's a simple way to avoid the issue altogether. In a nutshell, iOS 8 has a huge bug that has impacted several users who perform a reset on their devices using iOS's "Reset All Settings" function. In performing the wipe, some users have found that all of their documents stored in iCloud drive are getting deleted and then, since iCloud syncs to all devices, those documents are in turn being deleted off of connected iPads and Mac computers. Apple's latest iOS 8.0.2 update does not resolve the issue, so Wired notes that the best option is simply to embrace it. If you've already performed a reset and lost all of your documents, contact Apple support — it's your only hope. If you have not but you're planning to perform a device reset, go into it assuming that your iCloud Drive documents will be lost. Back them up to a Time Machine, another cloud service like Dropbox, or save them in a separate folder on your computer. Then, once the reset is complete, re-sync your documents if they were deleted. To read more click **HERE**