Counterintelligence New Mexico Working Group
NMCIWG Purple Arrow

The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
28 February 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

February 27, Softpedia – (International) **Fake "payment certificate" notifications used to deliver cross-platform RAT.** Symantec researchers reported a spam campaign designed to distribute the Java remote access trojan (RAT) dubbed JRAT that is cross-platform, potentially infecting machines running Windows, OS X, and Linux operating systems. Source: http://news.softpedia.com/news/Fake-Payment-Certificate-Notifications-Used-to-Deliver-Cross-Platform-RAT-429736.shtml

February 27, Network World – (International) **Security firm discloses Apple iOS 'malicious profile' vulnerability impact on MDM.** Apple will release a patch addressing a vulnerability disclosed by researchers in Apple iOS devices that can impact mobile-device-management (MDM) systems running on them by allowing an attacker to create a hard to detect malicious profile hidden on the device. Source: http://www.networkworld.com/news/2014/022714-rsa-skycure-279094.html

February 27, Softpedia – (International) **Flaws in Amazon's mobile apps could have been exploited to crack passwords.** Amazon patched their server after FireEye researchers reported that a weak password policy and no limitation or CAPTCHAs for passwords attempts could have been exploited by attackers to crack the passwords of accounts. Source: http://news.softpedia.com/news/Vulnerabilities-in-Amazon-s-Mobile-Apps-Could-Have-Been-Exploited-to-Crack-Passwords-429664.shtml

February 27, Softpedia – (International) **Three alleged hackers arrested in Korea for stealing information from hundreds of sites.** Three individuals from Korea are suspected of hacking into 225 Web sites and stealing the personal details of 17 million individuals including, real estate and trading services, Korean medical associations, and online gambling sites. Source: http://news.softpedia.com/news/Three-Alleged-Hackers-Arrested-in-Korea-for-Stealing-Information-from-Hundreds-of-Sites-429630.shtml

February 27, Softpedia – (International) **D-Link fixes persistent SSL certificate vulnerability in DCS IP cameras.** Firmware updates for several D-Link surveillance camera models from the DCS series were released addressing a SSL certificate vulnerability that could have allowed a malicious user to potentially gain access to the camera control information. Source: http://news.softpedia.com/news/D-Link-Fixes-Persistent-SSL-Certificate-Vulnerability-in-DCS-IP-Cameras-429622.shtml

February 26, Threatpost – (International) **Avaya to patch zero days that turn IP phone into radio transmitters.** Avaya will release a patch for two zero-day vulnerabilities in its latest one-X 9608 IP telephones that allow bugs to be exploited remotely, bypassing security appliances used to scan for malicious outgoing network traffic and allow the IP phone to turn into a transmitter. Source: http://threatpost.com/avaya-to-patch-zero-days-that-turn-ip-phone-in-radio-transmitters/104506

Your information for sale: the illicit online marketplace

Yahoo, 27 Feb 2014: Adding to an endless series of reports on Internet security breaches, cybersecurity firm Hold Security LLC revealed this week that it discovered stolen credentials from some 360 million accounts available for sale on the underground Internet. Although it's unclear now where the attacks were focused, the information unearthed includes user names and largely unencrypted passwords that could lead to anything from online bank accounts to huge corporate networks. Hold Security last year uncovered a massive hack at Adobe Systems that surfaced tens of millions of email addresses and encrypted passwords; this latest breach reportedly includes one attack that alone yielded more than 100 million records. Welcome to the shadowy "deep Web," where, along with drugs, weapons and hit men, one can purchase access to credit cards, online bank accounts, personal and corporate email accounts, health insurance information and much more. A "shopper" with $200 can buy a premium credit card number, secure a Gmail account or even rent a botnet that can infect networks of computers and be used to spread spam, launch denial of service attacks to major websites, attack bank computers and more. Those looking to purchase these items use tools such as Tor, which includes an identity-masking browser. Yahoo Finance took a virtual shopping trip to browse what was available for purchase at this vast illicit Internet mall (naturally, we were just looking — not buying). The sales here can come and go very quickly, and items are often priced by the level of difficulty attached to obtaining them (for example, stolen health insurance information can go for as much as $1,300 a pop). To read more click **HERE**

41% of British CryptoLocker Victims Sent Money to Cybercriminals

SoftPedia, 28 Feb 2014: The University of Kent has conducted a second cyber security study. The results (**link**) show that many people in Britain agree to pay up after their computers are infected with ransomware. 9.7% of the 1,502 respondents admitted falling victim to ransomware – some to the notorious CryptoLocker, while others to "police ransomware." Around 41% of those who have fallen victim to CryptoLocker have admitted paying the ransom to recover their files. As far as other types of ransomware are concerned, 30% admitted paying up. Interestingly, these findings are in contrast with the ones of Symantec and Dell SecureWorks, which have reported that only 3%, respectively 0.4%, of victims have agreed to pay the ransom. While University of Kent researchers highlight that the results might not be very accurate because of the size and bias of the sampled population, the difference is remarkably high. "If this were true and other researchers' findings corroborate this figure in the future, it shows a lack of success of the multiple public calls discouraging victims to pay the ransom, and would explain the enormous success of this particular ransomware (from the criminals' point of view, of course) and why copycats are rapidly emerging," the study reads. In addition to ransomware, the report also analyzes other aspects of cyber security. For instance, researchers have found that only 6.6% of respondents don't feel they're at risk of becoming victims of cybercrime. Over one quarter of those who took part in the study admitted falling victim to cyber-dependent crime over the last year. When it comes to cyber-enabled crimes, such as cyberbullying, 11% confirmed being victims over the last 12 months. When asked about whom they reported cybercrimes to, 5% said they alerted a financial institution. 3.8% reported the crime to their Internet service provider. Unfortunately, very few have filed reports with Action Fraud, which is the UK's national fraud reporting center, or law enforcement. "These troubling findings indicate a low level of awareness on how and whom to report experiences of cybercrime to, highlighting the sore need for increased awareness among the general population covering the different options for properly reporting a cybercrime," the university's report reveals. 13% of respondents said they didn't report the crimes to anyone because they either didn't know who to turn to, or they simply thought it would be a waste of time. To read more click **HERE**

Windows Security Flaws Doubled in 2013, Windows 8 the Most Vulnerable OS

SoftPedia, 27 Feb 2014: Microsoft has worked a lot to make Windows 8 and 8.1 more secure, but according to a new research rolled out by Secunia today, Windows vulnerabilities doubled last year, and the modern OS version was the most vulnerable of all editions still supported right now. The security company found more than 350 vulnerabilities in Windows XP, 7, and 8 in 2013, with statistics confirming that, despite all improvements made by Microsoft, the final numbers doubled compared to 2012 figures. Overall, Windows 7 had a total of 102 vulnerabilities, up from 50 in 2012, while Windows XP, which is said to become a very unsecure platform in just one month, had only 99 security flaws, an increase from 49 the year before. Windows 8, on the other hand, was pretty much the most vulnerable Windows version still supported by Microsoft, with Secunia pointing to a total of 156 glitches found in this particular build. And still, the platform itself is not at fault, Secunia said, as the integration of Adobe's Flash Player in Internet Explorer was the main reason why so many flaws have been reported in Windows 8.   Internet Explorer 10, which is the default browser in Windows 8, comes with built-in Flash Player support, which means that Microsoft needs to work with Adobe and patch the browser itself whenever a flaw is found in the application. Fixes are often delivered on Patch Tuesday, along with other improvements for Microsoft products.   Every Windows version still supported by Microsoft had more than 1200 total vulnerabilities in 2013. Microsoft programs and third-party applications still supported by the company had more than 1,200 security flaws last year, with Windows 8 again the leader, with 1,261 records. Of course, even though so many vulnerabilities have been reported in Windows operating system, this doesn't necessarily mean that users were open to attacks or some have fallen victims to hackers. In fact, Microsoft has until now managed to deal with all these security glitches pretty decently, with only a limited number of exploits found out there in the wild and obviously a reduced number of users getting hacked until the company actually shipped the patches to users. Windows 8 continues to be the most secure OS version to date and, with Windows XP's end of support quickly approaching, there's no doubt that all users need to reconsider their options and pick their next OS version as soon as possible. To read more click **HERE**