THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

24 September 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 23, Securityweek – (International) **Serious vulnerabilities found in wireless thermostats.** Researchers found that UK-based Heatmiser Wi-Fi thermostats contain at least nine vulnerabilities that can be controlled remotely by forwarding port 80 for Web control and port 8068 for mobile apps. Heatmiser announced that it is looking into the findings and recommended customers close port 80 on their thermostats. Source: http://www.securityweek.com/serious-vulnerabilities-found-wireless-thermostats

September 23, Techworld – (International) **DDoS attackers turn fire on ISPs and gaming servers.** NSFOCUS researchers determined gaming hosts and Internet service Providers (ISP) have been the focus for distributed denial of service (DDoS) attacks in 2014, rising in the first half to 10 percent and nearly 15 percent of attacks respectively. Source: http://www.networkworld.com/article/2687127/security/ddos-attackers-turn-fire-on-isps-and-gaming-servers.html

September 23, Help Net Security – (International) **jQuery.com compromised to serve malware via drive-by download.** RiskIQ researchers found and reported that jQuery.com, the official Web site of the cross-platform JavaScript library of the same name, was compromised and redirected its visitors to a site hosting the RIG exploit kit and delivered information-stealing malware. The attack was discovered September 18 and the site's administrators removed the malicious script. Source: http://www.net-security.org/malware_news.php?id=2869

September 22, Threatpost – (International) **Kyle and Stan malvertising network nine times bigger than first reported.** Researchers found nearly 6,500 malicious domains are involved in the Kyle and Stan malvertising network and over 31,000 connections were made to the domains, nine times larger than originally reported by Cisco. The campaign is unique in its ability to infect Windows and Mac OS X software differently and can drop ads on larger Web sites. Source: http://threatpost.com/kyle-and-stan-malvertising-network-nine-times-bigger-than-first-reported

Home Depot Hack Is Letting Criminals Drain Money from People's Bank Accounts
Reuters, 24 Sep 2014: On Tuesday, Sept. 2, 2014, the home improvement retailer said that it's looking into "unusual activity" and that it's working with both banks and law enforcement after suspicions of a credit card data breach. Data breach at home improvement retailer Home Depot Inc has led to fraudulent transactions across the United States, draining cash from customer bank accounts, the Wall Street Journal said. Criminals are using stolen card information to buy prepaid cards, electronics and even groceries, the Journal said, citing people familiar with the matter. Financial institutions also are stepping up efforts to block the transactions by rejecting them if they appear unusual, the daily said. Earlier this month, Home Depot confirmed its payment systems were breached and said some 56 million payment cards were likely compromised in a cyberattack at its stores, suggesting the hacking attack at the home improvement chain was larger than last year's unprecedented breach at Target Corp. Home Depot had said customers who shopped at its stores as far back as April were exposed. To read more click **HERE**

Kali NetHunter turns Nexus devices into portable hacking tools

Heise Security, 24 September 2014: Offensive Security, the security training company behind Kali Linux, the popular Debian-based OS designed for digital forensics and penetration testing, and Kali community member "BinkyBear" have created another great tool for pentesters: NetHunter. "NetHunter is a Android penetration testing platform for Nexus devices built on top of Kali Linux," the company explained on the tool's official website. "Of course, you have all the usual Kali tools in NetHunter as well as the ability to get a full VNC session from your phone to a graphical Kali chroot." But the NetHunter OS also has additional features like pre-programmed HID Keyboard attacks (turns the device and its OTG USB cable into a pre-programmed keyboard), BadUSB Man In The Middle attacks, one-click MANA Evil Access Point setups (for performing Wi-Fi AP and MitM attacks), and so on. This is only the beginning, they say, as they hope to add new features with the help of the community. Those wishing to test NetHunter can do so immediately, as the tool is open source and free to use. The only thing that they must have to make it work as it should is a Google Nexus device (5, 7 or 10). The tool currently does not work well on non-Nexus Android devices, because it's designed to exploit specific kernel sources the team managed to get from Google. "It is possible to build 'rootfs' NetHunter images only, which don't include our custom kernel, so features like HID, Wi-Fi injection, and BadUSB will not work, and in general, 'Your Mileage May Vary', they explained. "We do not provide support for this though, so you're on your own." To read more click HERE

Companies becoming lax in managing BYOD risk

Heise Security, 24 Sep 2014: Exposure to risk is as much of a threat today as it was in 2013; however, organizations have become less diligent in BYOD management and mitigation, according to TEKsystems. Seventy-two percent of IT professionals believe that sensitive company data is at risk due to employees accessing information from personal devices. Nearly two-thirds of respondents (64 percent) state that either no official BYOD policy exists at their organizations and/or nothing at all has been communicated about BYOD. This has increased by 21 percent from 2013, when 43 percent identified the same lack of guidelines and best practices. Despite the fact that mobile devices provide IT professionals with greater flexibility, they also heighten stress and extend the workday.

- Half of respondents say the ability to access work (e.g., applications, documents, email) via a mobile device has increased stress because they are never able to disconnect. Only 28 percent feel it lessens stress and 22 percent report it has no impact on stress.
- Almost two-thirds (61 percent) of all respondents disclose that if they had their choice, they would prefer to work in yesterday's world where they would be inaccessible outside of business hours.
- Although the majority of respondents would like to be able to disconnect, they acknowledge that mobility gives them greater control over their work life. For many, there is also a sense of urgency about being connected.
- Sixty percent of respondents indicate mobility gives them greater control over their work life, while 28 percent indicate it gives the employer more control.
- Forty-two percent of respondents admit that even during off hours, if their smartphone lost the ability to connect to work, they would alert IT to the problem within one hour.
- When asked about their morning routine, 28 percent of IT professionals confess that the first thing they do when they wake up is check their mobile device—even before using the bathroom.
- Although it seems smart devices are gaining traction as the favored communication method, when it comes to core work activities, the laptop is still the preferred device.
- IT professionals report that the time they spend working on various devices during a typical business day (laptop 67 percent, smartphone 25 percent, tablet 8 percent) is nearly identical to the time spent working on those devices after-hours (laptop 61 percent, smartphone 31 percent, tablet 8 percent).
- Sixty-one percent of respondents say that if they had to pick only one device to access work after-hours for the period of one week, they would choose their laptop.

"The growing deficiency of BYOD policy and management uncovered in this snapshot is astonishing, especially given the heightened threats of cybercrime and mobile security attacks," says Jason Hayman, TEKsystems market research manager. "The degree of exposure to risk is amplified by the fact that IT professionals and other employees are always connected, working from multiple devices from just about any location. These findings suggest that companies have either become completely overwhelmed by the process of instituting and upholding BYOD controls, don't feel that there is a legitimate threat, or have made the dangerous assumption that their tech-savvy workforce doesn't need direction regarding safe use of personal devices." To read more click HERE

880,000 Customers of TripAdvisor's Viator Notified of Payment Card Breach

Softpedia, 24 Sep 2014: The computer systems of Viator, a TripAdvisor-owned website that offers tour-booking services for worldwide destinations, have been compromised and the incident exposed payment card information of 880,000 customers, fraudulent transactions occurring in the case of some of them. The total number of customers affected by the incident is much higher, reaching 1.440 million, as the perpetrators also accessed Viator account details in the case of 560,000 clients. The breach was made known to the company on September 2, and late last week, on September 19, an announcement was published informing users of the data compromise. Viator discovered the breach after their payment card service provider informed them that unauthorized charges were recorded for the credit cards of some of their customers. Following an investigation carried out by a team of forensic experts, the company determined that about 880,000 clients might have their payment card information compromised. This includes credit or debit card number, expiration date, name, billing and email addresses. Fortunately, Viator saved the card numbers in an encrypted form, although there are no details about the encryption algorithm used. Chris Boyd, malware intelligence analyst at Malwarebytes Labs, said via email that "if you haven't experienced a fraudulent transaction yet, you may be in the clear. Stolen payment data doesn't tend to get stockpiled for too long because the people sitting on it know it's only a matter of time before someone, somewhere notices and has the card cancelled." Web account details of more than half a million visitors of the website were also affected during the incident, as the company started to notify them that their email address, nickname and encrypted password may have been accessed without authorization by an unknown party. Users are advised to change their passwords on Viator and other websites, if the same one is used, to protect from illegal access to their account. On the same note, the company recommends monitoring the card activity and report fraudulent transactions to their credit card company. "Customers will not be responsible for fraudulent charges to their accounts if they are reported in a timely manner," the data breach disclosure says. Boyd said that there isn't evidence of a large database containing personally identifiable information being posted online, but this does not mean that it does not exist. "There doesn't appear to have been a massive file posted online yet containing data such as PII related to the compromise - while that doesn't mean there isn't one, it's a slim branch of hope to hold onto as we await more information on this latest high-profile attack," he stated. To read more click HERE

Two Jimmy John's restaurants in New Mexico are part of national data breach

KOB News, 24 Sep 2014: Two Jimmy John's restaurants located in New Mexico are part of national data breach targeting the sandwich shop giant. In a released statement, the company says it "learned of a possible security incident involving credit and debit card data at some of Jimmy John's stores and franchised locations." The breach took place between June 16 and Sept. 5. Jimmy John's released a list of around 216 affected stores, including the Albuquerque restaurant located at 6500 Holly Avenue NE and the Roswell restaurant located at 2810 N. Main St. The company is offering identity protection services to impacted customers. For more information, call (855)-398-6442. To read more click HERE