THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

4 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 3, Help Net Security – (International) **Cybercriminals love PayPal, financial phishing on the rise.** Kaspersky Lab researchers released statistics on spam and phishing emails for the month of July, which found that phishing emails targeting financial services increased 7.9 percent during the month, with PayPal being the most targeted company. The researchers also found that the overall share of spam in all email traffic increased 2.2 percent to a total of 67 percent during July, among other findings. Source: http://www.net-security.org/secworld.php?id=17320

September 3, Help Net Security – (International) **Linux systems infiltrated and controlled in a DDoS botnet.** Researchers at Akamai Technologies reported that Linux systems could be at risk of infections using IptabLes and IptabLex to compromise systems and use them in distributed denial of service (DDoS) attacks. The researchers reported that the infections appeared to be caused by a large number of Linux-based Web servers being compromised via Apache Struts, Tomcat, and Elasticsearch vulnerabilities. Source: http://www.net-security.org/secworld.php?id=17322

September 3, The Register – (International) **Firefox 32 moves to kill MITM attacks.** The Mozilla Foundation released version 32 of its Firefox browser, which adds new features including public key pinning to help protect users against man-in-the-middle (MitM) attacks. Source: http://www.theregister.co.uk/2014/09/03/firefox_32_moves_to_kill_mitm_attacks/

September 2, Threatpost – (International) **Apple fixes glitch in Find My iPhone app connected to celebrity photo leak.** A security issue in Apple's Find My iPhone app that researchers demonstrated could be exploited in brute force attacks was fixed by the company. Apple stated that a recent breach of celebrities' personal photos stored in its iCloud service was not the result of the researchers' findings, but instead involved targeted attacks on the individuals' accounts. Source: http://threatpost.com/apple-fixes-glitch-in-find-my-iphone-app-connected-to-celbrity-photo-leak

September 3, SecurityWeek – (International) **Goodwill blames credit card breach on third-party vendor.** Goodwill Industries International representatives reported September 2 that a payment card breach which was detected in July was the result of hackers using an unidentified piece of malware to breach the systems of a third-party vendor that processes payments for some Goodwill members between February 2013 and August 2014. Servers at 20 Goodwill stores across several States were compromised during the breach, and the personal information, including name and payment card information, of the stores' customers was accessed. Source: http://www.securityweek.com/goodwill-blames-credit-card-breach-third-party-vendor

September 2, Los Angeles Times – (International) **Home Depot probing possible hacking; customer data may be at risk.** Home Depot representatives announced September 2 that the company is investigating a potential security breach and are working with law enforcement and banking institutions to investigate reported unusual activity. Source: http://www.latimes.com/business/la-fi-home-depot-hack-20140902-story.html

9 ways to protect data on your smartphone

Heise Security, 4 Sep 2014: Recent headlines of Hollywood celebrities' nude photos leaking onto the Internet remind us of the privacy risks we face when we store personal data – particularly very personal data – on smart devices. Here are nine recommendations from Catalin Cosoi, Chief Security Strategist at Bitdefender:

- Avoid storing pictures locally on your laptop, smartphone or tablet. Last year, a total of 290,651 devices such as laptops, smartphones and tablets were reported stolen In the UK. Smartphone theft is so common that, in the US, all devices will be pre-equipped with anti-theft capabilities by next year.
- Keep secure backups on Hard Disk Drives or other less portable devices to securely store your confidential and sensitive documents. Make sure that the hard drive is kept well away from an internet connection, as any internet-connected device can be an open door for hackers at some point.
- Encrypt, encrypt, encrypt. It may seem an overhyped functionality, but making your data undecipherable to hackers is a strong defense. Latest generation Android devices have an embedded full-device encryption feature that can encrypt all data, including applications, downloaded files and pictures.
- Protect your accounts with strong, complex passwords. Use symbols, numbers and capital letters or even strange phrases to lock your cloud content from prying eyes.
- Try to blur out your face on potentially compromising images. You wouldn't want your risqué selfies to appear on Twitter, Reddit or Facebook would you?
- Don't email your private photos. Email accounts, especially those without two-factor authentication enabled, are easy targets for hackers looking to steal your personal details and intimate photos.
- Format your memory card or internal memory. When you sell or lend your phone, be sure to format and overwrite the data with a secure erase tool to make sure that nothing remains.
- Don't share confidential information on open Wi-Fi hotspots unless you use a proper mobile security solution to block unrequested connections. Hackers can monitor your traffic and grab your banking credentials and compromising pictures without your knowledge.
- Disable auto-uploads for cloud storage solutions such as iCloud and Dropbox. These services, as useful as they may seem, create cloud-based versions of your images without filtering your most sensitive files from the harmless ones.

To read more click **HERE**

80% of business users are unable to detect phishing scams

Heise Security, 4 Sep 2014: McAfee Labs revealed that phishing continues to be an effective tactic for infiltrating enterprise networks. Testing business users' ability to detect online scams, the McAfee Phishing Quiz uncovered that 80% of its participants failed to detect at least one of seven phishing emails. Furthermore, results showed that finance and HR departments, those holding some of the most sensitive corporate data, performed the worst at detecting scams, falling behind by a margin of 4% to 9%. Since last quarter's Threats Report, McAfee Labs has collected more than 250,000 new phishing URLs, leading to a total of nearly one million new sites in the past year. Not only was there an increase in total volume, there was a significant rise in the sophistication of phishing attacks occurring in the wild. Results showed both mass campaign phishing and spear phishing are still rampant in the attack strategies used by cybercriminals around the world. Meanwhile, the United States continues to host more phishing URLs than any other country. "One of the great challenges we face today is upgrading the Internet's core technologies to better suit the volume and sensitivity of traffic it now bears," said Vincent Weafer, senior vice president for McAfee Labs. "Every aspect of the trust chain has been broken in the last few years—from passwords to OpenSSL public key encryption and most recently USB security. The infrastructure that we so heavily rely on depends on technology that hasn't kept pace with change and no longer meets

today's demands." Findings also revealed new cybercrime opportunities since the public disclosure of the Heartbleed vulnerability, as stolen data from still vulnerable websites is currently being sold on the black market. Lists of unpatched websites have quickly become hit lists for cybercriminals and tools are readily available to mine unpatched sites. With these tools, it is possible to tie together an automated system that targets known vulnerable machines and extracts sensitive information. To read more click HERE

Network vulnerabilities IT admins can use to protect their network

Heise Security, 4 Sep 2014: Being able to adapt to change is one of the most important abilities in security today, mostly because attacks to defend against are able to do the same. The sophistication of current threats is mainly seen in their skill to adjust based on the weaknesses of the environment they are targeting. In this post, we will try to see networks the way attackers see them — through their vulnerabilities — and turn these around into guides for how IT administrators should protect their network.

- People are the weakest link: People will always remain vulnerable to external stimuli, especially those that trigger strong emotions. This is why social engineering will always be a part of attacks — there are a lot of techniques to be used, and a high probability of effectiveness. Embracing the assumption that people will always fall victim to social engineering attacks is important for IT admins simply because it is true. Network security needs to be designed with this in mind, regardless of how oriented the employees are. IT administrators can:
    - Configure the network to not only prevent attackers from getting into the network, but also from getting data out of it. This way, even if an attacker is able to gain control of a machine in the network, exfiltrating any stolen data will be difficult. A properly managed firewall and network access control would greatly help achieve this. Threat intelligence will also play a big part here, also, such as of IPs used as C&Cs in attacks.
    - Segment the network based on the level of security the systems need. Critical systems need to be isolated from the "normal" ones, either physically or through the network segment they are connected to.

      On top of these, however, employee education is still important and should be done regularly.
- The safest place is the most dangerous: Even the smallest of security gaps within the network can lead to the biggest of breaches. Attackers know this well, and it is important for IT admins to keep it in mind. The network should be audited on a regular basis to make sure that all areas are properly secured. For example, IT admins may not take into consideration that they themselves are potential targets, or that certain devices within the network can also be infection points such as the network printer or even the router. The same goes for web administrators. Attackers might not directly breach highly-secured sites such as banking websites, instead checking for other sites in the same DMZ (demilitarized zone), compromise them, and leverage the trust-relationship to conduct a side-channel attack against the banking website.
- People use weak passwords: It is no secret that password management is a challenge for most users, so working on the assumption that all members of the network have secure passwords is simply not an option. To secure the network under the assumption that users have insecure passwords would require the implementation of other authentication measures such as two-factor authentication or even biometrics.
- The network is haunted by ghost machines: All networks have ghost machines in them. These are the machines that are not found in the network topology map but are connected to the network. These may consist of employees' personal devices, external partners' devices, or machines that should be retired but aren't. Attackers leverage on these machines because they provide both access to the network and stealth. In order to counter this, IT administrators need to be keen on monitoring the systems that are connected to the network. They need to implement a Network

Access Control mechanism to monitor and control the level of access these ghost machines are entitled to in the network.

- Old vulnerabilities are reliable and can still be used: Assessing and addressing software vulnerabilities is a critical process for every IT administrator, and should always cover all bugs — both new and old. IT administrators need to keep in mind that a vulnerability will remain a threat to a network if not addressed, regardless of how long it's been since it was discovered.

To read more click HERE

Home Depot breached, carders selling stolen payment card info

Heise Security, 3 Sep 2014: The Home Depot, a popular American home improvement and construction retailer that boasts of 2,200 stores in the US and 287 abroad, has apparently suffered a data breach that compromised customer credit cards. The possibility was first flagged by Brian Krebs, who received word that two batches of credit and debit card information apparently stolen from the company is currently on sale on the infamous rescator(dot)com underground carder market. One batch seemingly contains card data of European users, the other that of US customers. "There are signs that the perpetrators of this apparent breach may be the same group of Russian and Ukrainian hackers responsible for the data breaches at Target, Sally Beauty and P.F. Chang's, among others," he noted. "It is not clear at this time how many stores may have been impacted, but preliminary analysis indicates the breach may extend across all 2,200 Home Depot stores in the United States." The alarm was first raised by several banks, who bought the card batches from the criminals and went through them to identify affected customers. They seem to believe that the breach may have initially happened in late April or early May 2014. If so, the crooks could have in their hands a number of cards that will greatly surpass the number compromised in the Target breach, Krebs noted. "We're looking into some unusual activity that might indicate a possible payment data breach and we're working with our banking partners and law enforcement to investigate," The Home Deport noted in a statement published on their website. "If we confirm a breach has occurred, we will make sure our customers are notified immediately." They also made sure to point out to the potentially affected customers that they will not be responsible for any possible fraudulent charges. "The potential breach at Home Depot feels like deja vu in the wake of Target's massive breach last year. The reported extent and timeline dating back to April and May of this year would indicate a similar type of incident to Target where attackers were able to get onto the network to siphon off large amounts of data without being detected," commented Eric Chiu, president and co-founder at HyTrust. "These breaches are no longer a security or IT issue, but rather a business issue given the potential of massive losses and brand damage. Consumers should be able to expect better security from us. Especially as organizations are hit with breaches similar to others in their same industry…and worse, one that follows a breach of their own systems." Philip Lieberman, CEO of Lieberman Software, said that he was not surprised this has happened. "We were in contact with them many years ago trying to convince them to implement automation technology to rotate their passwords, but they chose to implement a less expensive and inferior solution from an off-shore company. The rest of the targets in the listed article by Krebs purchased the same ineffective technology from the same off-shore company with similar results." "Organized criminal syndicates are actively targeting US retailers simply because they've become lucrative targets; these groups take advantage of inherent vulnerabilities in payment architectures and applications, amongst other tactics, to get into these retail chains and siphon data off undetected," Ken Westin, security analyst at Tripwire, pointed out. "There's little that consumers can do directly to protect themselves from these sort of compromises," concluded Patrick Thomas, security consultant at Neohapsis. "Certainly all consumers should keep a close eye on their credit card statements and credit report, but they can also vote with their dollars and reward companies that publicly demonstrate a commitment to security." To read more click HERE