THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

22 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

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

Hackers Steal Usernames and Passwords of 5,000 Government Recruiters from NSA and Other Services

The Daily Caller, 18 Sep 2014: Hackers responsible for stealing the account information of 5,000 government recruiters on GovJobs.com may be preparing to impersonate recruiters and gain access to classified information with the credentials of clearance-holding job seekers. California security firm IntelCrawler discovered the security compromise of usernames, emails and passwords belonging to recruiters from every military service, multiple government agencies including NSA and some of the government's top defense contractors. IntelCrawler President Dan Clements told Bloomberg that "[h]ackers with such information could impersonate recruiters and tap job seekers who have knowledge of sensitive government projects, or seek damaging information about applicants to blackmail them into spying for them." According to the company, hackers could compare lists of job hunters against earlier hacks of commercial companies in order to obtain blackmail-worthy information belonging to government workers. IntelCrawler said that some recruiters recycle passwords across multiple government worksites and contracts, potentially jeopardizing their contacts beyond the compromised accounts that have been identified. The breach occurred on Aug. 13 and the company has since reported their findings to Homeland Security's U.S. Computer Emergency Readiness Team, which is investigating the hack. To read more click **HERE**

NIST offers help in securing printers, copiers, scanners from cyber intrusions

Government IT, 15 Sep 2014: Individuals and organizations shouldn't just worry about protecting their computers connected to the Internet from cyber threats and attacks. They also need to worry about the potential for printers, copiers and scanners being hacked. The National Institute of Standards and Technology recently released draft guidance (pdf) pointing out the risks and vulnerabilities of so-called replication devices, which increasingly also include 3D printers and scanners. Besides reminding people about potential cybersecurity problems, it offers advice on how such devices and information that's stored or transmitted can be better protected. The agency is seeking public feedback on the document by Oct. 17. Historically, people and organizations didn't have to worry about threats to such devices because these machines were limited to basic copying, scanning and printing. Storage capability within them largely didn't exist and these devices were either connected directly to computers with a cable or were standalone. Now, most are connected to networks and they can be accessed and managed remotely. However, they're potentially subject to the same cyber problems – denial-of-service attacks, spam, hacking, and data theft, among others – as networked computers connected to the Internet. "A compromise may affect the confidentiality, integrity, or availability of both the device and the information it processes, stores, or transmits," according to NIST's draft guidance. Replication devices might transmit unencrypted data, which could be stolen or changed. They might have open ports and protocols that could allow attackers undetected access. Plus, anyone with permission to access such machines could install malware or get into other areas of a network. The agency said it's important to consider a replication device's capabilities and security features, among other things, as an organization manages its own security risks. The document presents issues and questions that organizations should consider related to device acquisition, implementation, operation and maintenance, and disposal as well as service lease agreements. To read NIST's draft guidance on replication device security click **HERE**. To read more click **HERE**

Apple could face heat from police on refusing data access, expert says

Reuters, 18 Sep 2014: Apple's tight privacy strategy on devices running its iOS 8 operating system will make life more difficult for law enforcement, warns one retired police official. "It absolutely puts another hurdle in the path of law enforcement," Raymond Foster, a retired LAPD lieutenant, told FoxNews.com, adding that the tech giant may face pushback from law enforcement agencies. "Apple could ultimately, if someone decides that it's enough of a problem, face legislation saying 'you can't do that.'" In a privacy statement on its website, Apple explains that customer data such as photos, messages, email, contacts and call history is protected by each individual's passcode on iPhones and iPads running iOS 8. "Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data," it says. "So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8." Foster, author of the book "Police Technology," notes that critical evidence such as a drug dealer's accounts or child pornography, is often held on mobile devices such as smartphones. Apple says that 93 percent of the requests it receives from law enforcement come in the form of a "device request," where officers are working on behalf of a customer to locate a stolen device. According to Apple, just 7 percent of the requests it receives are "account requests," where law enforcement is seeking customer account information. Less than 0.00385 percent of Apple customers have had data disclosed due to government information requests, according to the statement. However, the statement provides little clarity on how Apple handles national security requests. The Cupertino, Calif.-based firm notes that national security-related requests are not considered either device or account requests, and "are reported in a separate category altogether." Apple's iOS 8 privacy move will not impact police wiretapping efforts, according to Foster. "What Apple is doing in no way affects wiretaps, because the wiretap goes to the service provider," he said. "They are not a service provider, they are a device provider." Civil liberties groups have welcomed Apple's stance, which comes hot on the heels of the cyberattack that targeted the iCloud accounts of celebrities such as Jennifer Lawrence and Kate Upton. Apple subsequently strengthened its iCloud security, although CEO Tim Cook blamed the attack on a phishing scam, as opposed to a weakness in the company's systems. To read more click **HERE**

Windows Server 2003: Preparing the World for a New Windows XP Moment?

SoftPedia, 18 Sep 2014: Windows Server 2003 support will come to an end on April 14, 2015, and security experts warn that the world could get through another "Windows XP moment" unless organizations running it prepare for the transition to another platform. Microsoft ended Windows XP support on April 8, and although the company warned that sticking to an unsupported operating system was a very risky decision, approximately 25 percent of the desktop computers worldwide were still running it. That's very likely to happen with Windows Server 2003 as well, as only a few companies have until now expressed their intention to upgrade. As a result, David Mayer, practice director, Microsoft Solutions for Insight Enterprises, said in a statement for ChannelNomics that Windows Server 2003 end of support could affect even more people because it's running on servers critical for business operations. Many US companies still running it Microsoft isn't talking about the end of support of Windows Server 2003 as much as it did for Windows XP, but there's no doubt that organizations that are yet to upgrade must be aware of the approaching milestone. Mayer warns that security risks are getting bigger as we approach the deadline, so Windows Server 2003 customers have no other choice than to upgrade. To read more click **HERE**

Microsoft Removes another Broken Security Update

Softpedia, 18 Sep 2014: Microsoft's botched updates saga continues, this time with a patch that was designed for Lync Server 2010 and reportedly failing to install on a number of computers. Redmond has confirmed in an advisory released today that it decided to stop shipping the KB2982385 security update to users worldwide and at the same time to remove all links from the download center. At this point, it appears that the botched update wasn't causing too many issues to computers attempting to install it, but user complaints published online confirm that in most of the cases deployment fails with an error pointing out that the publisher of the driver cannot be verified. Not much is known now as to the number of

computers affected by the problem, but Microsoft has already started work on a fix and will re-release the update once it's ready. We're investigating, says Microsoft The software giant has already removed the download links of this bulletin to make sure that no other computer that might experience issues will receive it. The company has said in a statement that it's already looking into the problems, but has offered absolutely no timing details for the new patch. "Microsoft revised this bulletin to address a known issue that prevented users from successfully installing security update 2982385 for Microsoft Lync Server 2010. Microsoft is investigating behavior associated with the installation of this update, and will update this bulletin when more information becomes available. As an added precaution, Microsoft has removed the download links to the 2982385 security update," the company explains. Computers that managed to install the security update shouldn't do anything, even though it's also not clear whether some actually completed deployment of the patch. To read more click **HERE**

Home Depot Completes Malware Elimination, Says 56M Cards Were at Risk
Reuters, 18 Sep 2014: Home Depot Inc (HD) said on Thursday that data could have been stolen from 56 million payment cards by criminals who used malware from April to September to hack into its systems at stores in the United States and Canada. The world's largest home improvement chain said the malware, which was custom-built to evade detection, has been removed from its U.S. and Canadian stores. Home Depot started investigating the breach from Sept. 2 after security website Krebs on Security reported that all of the retailer's U.S. stores may have been affected by data theft. "We apologize to our customers for the inconvenience and 'anxiety this has caused and want to reassure them that they will not be liable for fraudulent charges," Home Depot's chairman and chief executive officer, Frank Blake, said in a statement. The company said it estimates costs related to the data breach, including providing credit monitoring services to its customers, increasing call center staffing, and the cost of legal and professional services, at $62 million, partially offset by reimbursable costs and insurance coverage totaling $27 million. / To read more click **HERE**

September 16, Associated Press – (National) **Probe: Healthcare.gov website must boost security.** The U.S. Government Accountability Office released a report September 16 stating that the Web site for the national healthcare program contained over 20 specific security issues related to who can access and make changes to the network. Representatives from the U.S. Department of Health and Human Services responded and stated that officials have acted on many recommendations provided in the report. Source: http://news.yahoo.com/probe-healthcare-gov-website-must-195439163.html

September 18, Help Net Security – (International) **Hackers penetrated systems of key defense contractors.** The computer systems of U.S. Transportation Command (TRANSCOM) contractors were successfully hacked by individuals associated with the Chinese government at least 20 times in one year, the Senate Armed Services Committee found. TRANSCOM was only aware of 2 intrusions but an investigation determined that in a 12-month period there were about 50 intrusions or other cyber-related events into their computer networks. Source: http://www.net-security.org/secworld.php?id=17375

September 18, Securityweek – (International) **Apple fixes "backdoors" with release of iOS 8.** Apple released the newest version of its mobile operating system, iOS 8, September 17, which adds improvements and closes over 50 security vulnerabilities. Source: http://www.securityweek.com/apple-fixes-backdoors-release-ios-8

September 17, Threatpost – (International) **Series of vulnerabilities found in Schneider Electric SCADA products.** An advisory from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned users of Schneider Electric StruxureWare SCADA Expert ClearSCADA products after researchers discovered unpatched, remotely-exploitable vulnerabilities. Included in the vulnerabilities is a cross-site scripting (XSS) issue that could allow industrial control systems (ICS) to be shut down, while an

authentication bypass issue could give attackers access to sensitive information. Source: http://threatpost.com/series-of-vulnerabilities-found-in-schneider-electric-scada-products

September 17, Securityweek – (International) **AppBuyer iOS malware targets jailbroken iPhones.** Researchers with Palo Alto Networks analyzed a piece of iOS malware discovered by WeiPhone Technical Group in May and found that the malware dubbed AppBuyer is targeting jailbroken iPhones in order to steal Apple ID and password information and make unauthorized purchases from the App Store. Source: http://www.securityweek.com/appbuyer-ios-malware-targets-jailbroken-iphones

September 17, SC Magazine – (International) **Analysts spot 'Critolock,' ransomware claims to be CryptoLocker.** Researchers at Trend Micro identified a new piece of ransomware known as Troj_Critolock.A or Critolock that infects devices and encrypts users' data and demands a ransom. The malware purports to be the CryptoLocker ransomware but contains several differences including its use of the Rijndael symmetric-key algorithm. Source: http://www.scmagazine.com/analysts-spot-critolock-ransomware-claims-to-be-cryptolocker/article/372182/

September 17, Threatpost – (International) **Drupal patches XSS vulnerability in spam module.** Drupal released a patch September 17 for the Mollom spam and content moderation module that closes a cross-site scripting (XSS) vulnerability that could allow an attacker to gain admin-level access to Web sites and enable them to steal data or hijack sessions. Source: http://threatpost.com/drupal-patches-xss-vulnerability-in-spam-module

September 18, Threatpost – (International) **Dyre trojan caught in the cookie jar.** An analysis by Adallom researchers found that a new variant of the Dyre banking trojan is targeting login credentials for large banks and corporate accounts. The new variant is capable of stealing client certificates and browser cookies, potentially acquiring the same account persistence for attackers as that held by legitimate users. Source: http://threatpost.com/dyre-trojan-caught-in-the-cookie-jar/108373

September 19, Securityweek – (International) **Apple fixes numerous vulnerabilities with release of Mac OS X 10.9.5.** Apple released the latest version of its OS X operating system September 18, which addresses over 40 vulnerabilities that could lead to information disclosure, arbitrary code execution, privilege escalation, and other issues. Apple also released security updates for its OS X Server, Apple TV, Xcode development platform, and Safari Web browser. Source: http://www.securityweek.com/apple-fixes-numerous-vulnerabilities-release-mac-os-x-1095

September 18, IDG News Service – (International) **Malicious advertisements distributed by DoubleClick, Zedo networks.** Researchers at Malwarebytes found that the DoubleClick and Zedo advertisement networks have been delivering malicious ads to several popular Web sites including Last.fm, The Times of Israel, and The Jerusalem Post. The malicious ads redirect users to a page hosting the Nuclear exploit kit which then attempts to drop the Zemot malware used by attackers to download additional malicious components. Source: http://www.networkworld.com/article/2686393/malicious-advertisements-distributed-by-doubleclick-zedo-networks.html

September 18, Reuters – (International) **Home Depot breach bigger than Target at 56 million cards.** Home Depot officials reported September 18 that 56 million payment cards were likely compromised when attackers used custom-built malware to breach the networks of stores in the U.S. and Canada between April and September 8 when the breach was detected. Costs associated with the breach are estimated to total $62 million to date. Source: http://www.reuters.com/article/2014/09/18/us-home-depot-dataprotection-idUSKBN0HD2J420140918

Payment card info of 880k Viator customers compromised

Heise Security, 22 Sep 2014: Payment card and personal information of approximately 1.4 million Viator.com customers may have been compromised in a breach that was confirmed late last Friday. The popular travel and tours provider has begun notifying customers of the breach. 880,000 customers may have had their payment card information (encrypted credit or debit card number, card expiration date, name, billing address and email address) and possibly their Viator account information (email address, encrypted password and Viator "nickname") compromised. "We have no reason to believe at this time that the three or four digit code printed at the back or front of customers' cards were compromised. Additionally, debit PIN numbers are not collected by Viator and could therefore not be compromised", the company made sure to note in the notice. Unfortunately, they didn't go into detail about the encryption used to protect the payment card information. Additionally, some 560,000 customers may have had their account information compromised. Not much is currently known about how the breach happened. "On September 2, we were informed by our payment card service provider that unauthorized charges occurred on a number of our customers' credit cards," the company simply stated. "We have hired forensic experts, notified law enforcement and we have been working diligently and comprehensively to investigate the incident, identify how our systems may have been impacted, and secure our systems." They advised all affected customers to monitor their card activity and report any fraudulent charges to their credit card company, and are offering free identity protection services for our customers in the US. Those outside the US might receive similar services once the company finds "appropriate comparable options." All customers are advised to change their Viator passwords, as well as the passwords on other sites where they used the same one. To read more click HERE

Home Depot security was anything but, say former employees

Heise Security, 22 Sep 2014: Bit by bit, information about the Home Depot security breach is coming to light, and the picture it paints is extremely unflattering for the retailer. The latest insight comes from former Home Depot IT employees and members of its cybersecurity team, who told the New York Times that the company was lax and slow-moving when it came to setting up defenses against cyber attackers. The company still uses Symantec antivirus software from 2007; does not perform network monitoring in order to spot unusual behavior; performs system and vulnerability scans irregularly and incompletely - the security staff was even not allowed to scan some systems handling customer information; and, finally, in 2012, the company employed a security engineer that was sentenced this April to four years in federal prison because he was found guilty of disabling the computers of his previous employers. Most of these former employees left the company of their own accord, after their requests for new software and training were repeatedly dismissed by managers saying: "We sell hammers." The company's bigwigs have apparently been galvanized into doing something only after the Target breach. Home Depot CEO reacted by setting up a team to protect the company's networks, and has called in outside experts from Voltage Security to help with the introduction of enhanced encryption for payment data. Unfortunately, the move came to late, as the attackers were already inside. Despite Home Depot's recent statement that "the hackers' method of entry has been closed off, the malware has been eliminated from the company's systems, and any terminals identified with malware were taken out of service," the ex-employees' insight into how information and system security was handled in the company should make us extremely skeptical about the retailer's claims. The attack against the company is estimated to have put at risk approximately 56 million unique payment cards, information of some of which is already being sold on carder forums. To read more click HERE

Home Depot completes malware elimination in all U.S. stores

Heise Security, 19 Sep 2014: Home Depot confirmed that the malware used in its recent breach has been eliminated from its U.S. and Canadian networks. They completed a major payment security project that provides encryption of payment data at point of sale in the company's U.S. stores, offering. Roll-out of enhanced encryption to Canadian stores will be complete by early 2015. Canadian stores are already enabled with EMV "Chip and PIN" technology. The company's investigation has determined the following:

- Criminals used unique, custom-built malware to evade detection. The malware had not been seen previously in other attacks, according to Home Depot's security partners.
- The cyber-attack is estimated to have put payment card information at risk for approximately 56 million unique payment cards.
- The malware is believed to have been present between April and September 2014.

The hackers' method of entry has been closed off, the malware has been eliminated from the company's systems, and any terminals identified with malware were taken out of service. There is no evidence that debit PIN numbers were compromised or that the breach has impacted stores in Mexico or customers who shopped online at HomeDepot.com or HomeDepot.ca. To read more click **HERE**