THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

2 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

August 29, Softpedia – (International) **New BlackPoS strain disguises as antivirus service.** Researchers with Trend Micro identified a new variant of the BlackPoS point-of-sale (PoS) malware that disguises itself as an antivirus product and contains other changes to improve efficiency and avoid detection. The malware can reach PoS systems by the infection of company servers, breaching network communication, or infecting the PoS device before deployment. Source: http://news.softpedia.com/news/New-BlackPoS-Strain-Disguises-As-Antivirus-Service-456982.shtml

August 29, Softpedia – (International) **Hackers steal customer payment data from ClamCase.** Keyboard and iPad case manufacturer ClamCase stated that attackers compromised the company's systems and obtained an undisclosed number of customers' personal information including names, addresses, and payment card data. The company stated that the attack occurred between April 15 and August 6 and is offering identity theft prevention services to affected customers. Source: http://news.softpedia.com/news/Hackers-Steal-Customer-Payment-Data-From-ClamCase-456961.shtml

August 29, The Register – (International) **KER-CHING! CryptoWall ransomware scam rakes in $1 MEEELLION.** Dell SecureWorks researchers published an analysis of the CryptoWall ransomware and found that it continues to be the largest ransomware threat, extorting at least $1 million from victims. The researchers detected around 625,000 systems infected with the ransomware between mid-March and late August, encrypting over 5.25 billion files, among other findings. Source: http://www.theregister.co.uk/2014/08/29/cryptowall_analysis/

August 29, Help Net Security – (International) **Phishers targeting crypto currency and retail sites.** The Anti-Phishing Working Group (APWG) released its report for the second quarter of 2014 (Q2) and found that the number of phishing attacks was the second-highest number since recording began in 2008, with online payment services and cryptocurrency sites being frequent targets, among other findings. Source: http://www.net-security.org/secworld.php?id=17308

August 28, Softpedia – (International) **Dairy Queen confirms breach of payment systems.** Dairy Queen officials confirmed that systems in a limited number of stores were infected with Backoff point-of-sale (PoS) malware, and customers' personal information, including payment card information, may have been exposed. Source: http://news.softpedia.com/news/Dairy-Queen-Confirms-Breach-of-Payment-Systems-456832.shtml

70% of IT pros experience weekly phishing attacks
Heise Security, 1 September 2014: 69 percent of IT professionals experience phishing attacks at least once a week, with customer data cited most often as the type of data attacked, followed by financial information, according to HP. Seven out of 10 attacks generated within the network perimeter stem from a malware-infected host highlighting the importance of taking a layered approach to security to block suspicious communications at every point on the network—from the perimeter to the core. "Organizations are increasingly challenged to protect their networks from advanced targeted attacks, in fact, it is likely that most environments have already been breached with systems infected by malware," said

Frank Mong,vice president, Solutions, Enterprise Security Products, HP. "It's important that IT professionals understand how attackers are trying to break through the network, and have confidence in their ability to mitigate attacks when every second matters." Based on the Ipsos Observer online survey of more than 200 IT professionals based in the United States, the study also yielded the following findings:

- Approximately six out of 10 attacks stem from malicious communication with the command and control site, and over half are taking advantage of a software vulnerability. Top threats relative to these new attacks are primarily within the data center, mobile and branch networks.
- Among the organizations surveyed, China is stated most often as a country of origin for external network attacks, followed by Russia and the United States.
- Eighty-five percent of survey respondents indicated concern for illicit file sharing and use of non-work-related applications; 63 percent are concerned with employees visiting adult-only websites on the corporate network.
- Roughly seven in 10 claim that social media is a type of abuse occurring on their corporate network.
- In the event of a network breach, 67 percent of survey respondents listed customer data as the most likely to be attacked, followed by the company's financial information (63 percent). Other data at risk includes corporate intellectual property (59 percent) and employee data (49 percent).
- As companies look to adopt software-defined networking (SDN), 54 percent indicated network manageability as a top concern, while 44 percent are concerned with an attacker compromising the SDN controller.
- On average, enterprises are spending approximately $2.6 million annually on network security, and more than 60 percent of IT professionals surveyed expect to increase spending in the next year.

To read more click **HERE**

JPMorgan attackers altered bank records

Heise Security, 29 Aug 2014: The number of US banks that have apparently been targeted and breached by hackers is slowly rising, as newer reports say that seven financial organizations have been hit. Unnamed sources also say that the scope of the attacks is also larger than initially thought, as JPMorgan reported that the attackers changed and deleted some bank records. According to security and banking experts, cyber crooks have been known to do things like that, albeit rarely. According to Adam Kujawa, head of Malware Intelligence at Malwarebytes Labs, it's unlikely that the attackers are "average criminals." "If hackers are capable of accomplishing this, it means they have spent a significant amount of time studying the [bank's] records system before attempting any kind of serious manipulation," he commented for Cnet. "It's not impossible, however, if they were able to modify records using high-level credentials and do it in a way that was undetected." As the names of the other victimized financial institutions have not been publicly shared, customers of all US banks should be on the lookout for unusual activity in their accounts, and carefully peruse each email received from their bank, as it might be a fake. A short time before the breaches were uncovered, JPMorgan customers were at the receiving end of expertly crafted malicious emails purportedly sent by the bank. To read more click **HERE**

DHS urges website admins to minimize risk of Google hacking

Heise Security, 28 Aug 2014: It's a widely known fact that Google Search is a valuable tool for attackers looking for a way into organizations' information systems. "Google hacking" has been used for years by penetration testers and security researchers. Ars Technica reports that the US Department of Homeland Security and the FBI has recently sent out a notification to police, public safety and security personnel, warning them about "Google dorking", i.e. hacking. "By searching for specific file types and keywords, malicious cyber actors can locate information such as usernames and passwords, e-mail lists, sensitive documents, bank account details, and website vulnerabilities," the alert explains. "For example, a simple operator:keyword syntax, such as filetype:xls intext:username in the standard search box would retrieve

Excel spreadsheets containing usernames. Additionally, freely available online tools can run automated scans using multiple dork queries." The notice also mentions two instances when "dorking" was used to breach websites, and alerts readers to the existence of the Diggity Project, a free penetration testing tool suite that allows users / attackers to automate Google dork queries. Google hacking would not be such a successful technique if site owners and administrators took care to secure their websites, but the reality is that many don't, and occasionally should be reminded to do it. To read more click **HERE**

Extracting encryption keys by measuring computers' electric potential

Heise Security, 22 August 2014: A group of researchers from Technion and Tel Aviv University have demonstrated new and unexpected ways to retrieve decryption keys from computers. Their research is "based on the observation that the 'ground' electric potential in many computers fluctuates in a computation-dependent way." "An attacker can measure this signal by touching exposed metal on the computer's chassis with a plain wire, or even with a bare hand. The signal can also be measured at the remote end of Ethernet, VGA or USB cables," they explained. "Through suitable cryptanalysis and signal processing, we have extracted 4096-bit RSA keys and 3072-bit ElGamal keys from laptops, via each of these channels, as well as via power analysis and electromagnetic probing." Their attacks have been leveraged against GnuPG, and they used several side channels to do it. They measured fluctuations of the electric potential on the chassis of laptop computers by setting up a wire that connected to an amplifier and digitizer. They also found a way to measure the chassis potential via a cable with a conductive shield that is attached to an I/O port on the laptop. Most surprisingly, the signal can also be measured after it passes through a human body. Finally, they also succeeded in extracting the keys by measuring the electromagnetic emanations through an antenna and the current draw on the laptop's power supply via a microphone. The bad news is that each of these attacks can be easily and quickly performed without the user being none the wiser (the researchers included realistic, every-day scenarios in the paper). More information about the attacks can also be found here. To read more click **HERE**

Card PIN Codes Revealed by Finger Heat Signature

SoftPedia, 2 Sep 2014: A smartphone equipped with an infrared camera may become the pickpockets' favorite tool, as the kit can be used to detect the PIN code entered on PoS systems keyboards after the victim completes the transaction in a store. Objects emit light based on the temperature they produce, and this can be caught by infrared cameras. Since during the interaction between two objects heat is exchanged, the PIN key presses can be revealed by the heat signature left behind by the finger. Amazing as this may sound, such technology has been created to a scale so small that it can be integrated into a smartphone case, offering the convenience of portability. FLIR One is a device that attaches to an iPhone 5 or 5s and allows capturing the heat signatures of different objects. Blogger Mark Robber posted a video of him using the FLIR case to steal the PIN code of someone making a card transaction. He showed that by simply capturing the keypad of the PoS system with the infrared camera he was able to detect not just the numbers of the protective code but also their sequence, because of heat dissipation. During his tests, Robber says that the thermal signature persists for some time, and even if the chances of guessing the correct order dwindle as time passes, there is still at least a 50% chance to get the PIN accurately a minute after the victim enters the PIN. In the scenario presented by Robber there is no need for a full minute to pass in order to capture the keypad of the payment system. Given that the infrared camera is attached to a phone, the device can be held casually over the pad in order to capture the heat signature. The good news is that by simply resting some of the fingers on the keypad while entering the PIN, the heat exchange that occurs can mask the actual keys, eliminating the risk. Also, the method does not work on all PoS systems, since some of them have keypads made of materials that can dissipate the heat very quickly; metal keys on ATM machines fall into this category. However, most PoS systems have plastic keys that can retain heat and offer thieves the possibility to capture the security code and leave the task of lifting the wallet with the card to accomplices that could follow the victim outside the store and pickpocket them. On the bright side, the accessory is pretty expensive ($349 / €266) and it is currently

available only in the US. Such an investment could prove too costly for most pickpockets. To read more click HERE

Poor WPS Implementation in Routers Makes Devices Vulnerable to Offline Attacks

Softpedia, 2 Sep 2014: Routers that have a weak implementation of the WiFi Protected Setup (WPS) security standard are vulnerable to a new type of offline attack that could offer access to the network in seconds. A brute-force attack would reach the same end in a few hours, but the new one, presented by reverse engineer Dominique Bongard from 0xcite, requires a single guess to uncover the correct PIN code for accessing the device's WPS functions. The method used by the researcher relies on exploiting weak randomization in keys used for the authentication of hardware PINs. This is not possible in all implementations of WPS, but Bongard discovered that the issue was common to Broadcom chipset manufacturer and to another, undisclosed one. Devices with WPS enabled allow users to provide the WiFi Protected Access (WPA) passphrase to stations based on the right PIN code, making it easier to offer access to a protected network. WPS uses two main methods for adding devices to the network: one relies on pushing a button available on the device and another on entering an 8-digit code present either on a label on the device or in the documentation from the manufacturer. In the attack described by Bongard, the PIN is calculated offline, which means that a security measure, like limited attempts, becomes completely inefficient. Manufacturers rely on standard code for the custom router software, thus perpetuating the problem to the final product. According to Bongard, the code from Broadcom had weak randomization of the numbers. With the second vendor, the issue is even more severe, because there is no randomization at all. In a statement to Ars Technica, Carol Carrubba, spokeswoman for Wi-Fi Alliance, who introduced the standard in 2006, said that "it is likely that the issue lies in the specific vendor implementations rather than the technology itself. As the published research does not identify specific products, we do not know whether any Wi-Fi certified devices are affected, and we are unable to confirm the findings." The previous attack that broke WPS consisted in reducing the possible combinations of the brute-force attack to only 11,000 guesses, which can be done in a matter of hours (less than four). Regardless of the method used, the only way to prevent against this flaw is to disable WPS functionality altogether. According to the researcher, the prevalence of the problem is difficult to determine because many of the implementations are the reference code for the chipset; but, at the same time, plenty of vendors employ different chipsets, even for the same model number. To read more click HERE

Apple's iCloud Breach Is "Actively Investigated"

Softpedia, 2 Sep 2014: The news that a group of celebrities got their private pictures stolen and published only spread immediately on Monday. Anonymous posts on the website 4Chan got everyone's attention. The photos were allegedly taken from celebrities' iCloud accounts. It is believed that all the hacked accounts were using the Photo Stream feature and they have all been taken down using the brute force attack method. So far there's no confirmation that Apple's security in iCloud or other similar apps that use the same account have been compromised. In one instance, the photos had in the same folder with them a "Welcome to Dropbox" file that may mean everything started from Dropbox. All day on Monday, Apple has declined to comment on this situation, but early on Tuesday, their spokeswoman Natalie Kerris came with a message from Cupertino via Re/Code, "We take user privacy very seriously and are actively investigating this report." No word on whether this is an iCloud problem or something else coming from the same family of apps. There were voices on the Internet that explained how bad that could prove for Apple because they have Cloud Kit and iCloud drive coming with iOS 8. Also, Apple is offering a new app for its users, Health.app. This will track your burned calories, running schedule and bodily functions all in one and report it to a doctor or a Medical Center. Everything was believed to be secure, until people started finding the nude pictures released a day ago. Would you trust your private life to the Cloud? To read more click HERE

FBI, NSA Investigating Whether Russia Hacked U.S. Banks to Retaliate for Sanctions

Daily Caller, 27 Aug 2014: The FBI suspects an earlier August cyberattack on the U.S. financial system, which resulted in the theft of data from JPMorgan Chase, may have been the work of Russian hackers retaliating for U.S.-imposed economic sanctions. Citing "people familiar with the probe," Bloomberg reports the sophisticated nature of the attack along with evidence pulled from bank computers points to a Russian government link. The hack, which exploited a vulnerability on a bank website, broke through multiple layers of complex security to steal gigs of sensitive data from JPMorgan and at least one other, unnamed bank. Data seized from bank employees — including executives — may have included customer data. Security experts cited in the report said the hack executed was too complicated and precise to be attributed to average non-state-sponsored criminal hackers, but investigators haven't ruled out the possibility of cyber criminals in Russia or elsewhere in Eastern Europe. Investigators are also considering whether the recent hack of large European banks, which took advantage of a similar vulnerability, are linked to the August breach. The National Security Agency has also joined the investigation. According to the report, cyberattacks against the U.S. financial system traced to Russia and Eastern Europe have amped up in the months since President Barack Obama authorized economic sanctions against Russia for its support of rebels in Eastern Ukraine, and the annexation of Crimea. JPMorgan was the target of criticism from Russia's foreign ministry in April, when the bank blocked a payment from a Russian embassy to a U.S.-sanctioned bank affiliate — a move Russia called "illegal and absurd." To read more click **HERE**