THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

17 June 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

June 16, Threatpost – (International) **Dyreza banker trojan seen bypassing SSL.** Researchers identified a new banking trojan known as Dyre or Dyreza that uses browser hooking to intercept traffic moving between victims' systems and their intended Web site, allowing attackers to bypass SSL protections and redirect traffic through the attackers' servers. Researchers at CSIS Group found that the trojan is spread through spam messages and then contacts command and control servers, some of which are located in Latvia. Source: http://threatpost.com/dyreza-banker-trojan-seen-bypassing-ssl/106671

June 14, Krebs on Security – (National) **P.F. Chang's confirms credit card breach.** P.F. Chang's Chinese Bistro stated June 14 that it had confirmed that it was the victim of a customer payment card data breach affecting an unknown number of customers. The company stated that it has temporarily switched to manual payment card imprinting to process transactions while the breach continues to be investigated. Source: http://krebsonsecurity.com/2014/06/p-f-changs-confirms-credit-card-breach/

June 16, Softpedia – (International) **NAS boxes "pwned" by crypto currency miner.** Researchers with Dell SecureWorks released a report which showed how an attacker was able to utilize vulnerabilities in the DiskStation Manager (DSM) operating system used in Synology network access storage (NAS) devices to plant the CPUMiner crypto currency mining malware. The attacker used the malware to mine over $600,000 in the Dogecoin crypto currency, though the vulnerabilities were later patched by Synology. Source: http://news.softpedia.com/news/NAS-Boxes-Pwnwed-by-Crypto-Currency-Miner-446883.shtml

June 13, Threatpost – (International) **ISC patches critical DoS vulnerability in BIND.** The Internet Systems Consortium (ISC) reported June 11 that a vulnerability exists in some BIND domain name system (DNS) servers that could allow attackers to perform denial of service (DoS) attacks by sending a specially designed query. The ISC advised users to update to the newest version of BIND, which is not vulnerable. Source: http://threatpost.com/isc-patches-critical-dos-vulnerability-in-bind/106653

Comcast is turning your home router into a public Wi-Fi hotspot
CNN, 16 Jun 2014: If you're a Comcast cable customer, your home's private Wi-Fi router is being turned into a public hotspot. It's potentially creepy and annoying. But the upside is Internet everywhere. It's been one year since Comcast (CMCSA) started its monster project to blanket residential and commercial areas with continuous Wi-Fi coverage. Imagine waves of wireless Internet emitting from every home, business and public waiting area. Comcast has been swapping out customers' old routers with new ones capable of doubling as public hotspots. So far, the company has turned 3 million home devices into public ones. By year's end it plans to activate that feature on the other 5 million already installed. Anyone with an Xfinity account can register their devices (laptop, tablet, phone) and the public network will always keep them registered -- at a friend's home, coffee shop or bus stop. No more asking for your cousin's Wi-Fi network password. But what about privacy? It seems like Comcast did this the right way. Outsiders never get access to your private, password-protected home network. Each box has two separate antennae, Comcast explained. That means criminals can't jump from the

public channel into your network and spy on you. And don't expect every passing stranger to get access. The Wi-Fi signal is no stronger than it is now, so anyone camped in your front yard will have a difficult time tapping into the public network. This system was meant for guests at home, not on the street. Anyone hooking up to the "Xfinity Wi-Fi" public network must sign in with their own traceable, Comcast customer credentials. Still, no system is foolproof, and this could be unnecessary exposure to potential harm. Craig Young, a computer security researcher at Tripwire, has tested the top 50 routers on the market right now. He found that two-thirds of them have serious weaknesses. If a hacker finds one in this Comcast box, all bets are off. "If you're opening up another access point, it increases the likelihood that someone can tamper with your router," he said. What about connection speed? Having several people tapping a single machine tends to clog up the Wi-Fi. Comcast says it found a way to make this work. With two separate networks, each antenna has its own data speed cap. Comcast said the private channel provides whatever speed customers already pay to get (most have 25 Megabits per second). The public hotspot channel is given 15 Mbps and allows up to five people to connect at a time. That means having your data-hungry friends over shouldn't slow down your Netflix (NFLX, Tech30) stream. Comcast spokesman Charlie Douglas promised "there's more than enough capacity" in the cables connecting to people's homes to make this work. "You shouldn't experience any conflict between the two networks," he said. "It's something our engineers thought about carefully. The last thing we want to allow is to create a bad user experience." Comcast's project that started in northern New Jersey has now spread to Boston, Chicago, Houston, Indianapolis, Minneapolis, Philadelphia, San Francisco, Seattle and elsewhere. "Before this, there was no value in having Internet when you're not at home," Douglas said. "Every time you left the house you walked away from your subscription. But with all these hotspot locations, you can connect to the Internet remotely. Everyone's device is mobile. It makes a lot of sense." But what if you hate the idea of your private boxes turned into public hotspots? You can turn it off by calling Comcast or logging into your account online. The company says fewer than 1% of customers have done that so far. To read more click HERE

Five Things Facebook Knows About You

Wall Street Journal, 13 Jun 2014

1. Where You Browse: Using tracking cookies, Facebook is able to determine the sites you visit. If you browse for a fancy watch, you'll likely start seeing more watch ads. Facebook's mobile app can take stock of other apps you've installed, too. Facebook argues that ads are a better experience if they are about your interests.
2. What You Look Like: For many, Facebook has inadvertently become the cloud storage of choice for some of our most personal information — photos. Tagging someone tells Facebook you have a relationship. Facebook can recognize faces in photos and try to match them to other photos. Facebook isn't alone – Google acquired a facial-recognition company in 2011.
3. Where You Go: If you have Facebook's app open on a smartphone, Facebook can track your location and build a profile of where you live, work, shop and play. Facebook's "nearby friends" feature suggests when someone you know is nearby. Adding locations to status updates gives Facebook a better idea about your intent. Check in from ice-cream stores a lot? You're telling advertisers you have a sweet tooth.
4. Your Relationships: Facebook takes your big list of "friends" and categorizes them into family, friends from high school, colleagues and more. Apps within Facebook do this too. Many people willingly indicate their parents, siblings and significant others. The basic Facebook account can include your name, age, gender, birthday, family, places you have lived, employers and more. Facebook knows the people that you've searched for — and how often.
5. What You Are Interested In: Facebook prompts members to indicate their favorite movies, songs and more. Did you tell Facebook you like "Game of Thrones?" Then expect ads about fantasy books. If you opt in to a new feature, Facebook may figure out you are watching "Game of Thrones" by using your device's microphone and recognizing the theme song as you type a status

update. A lot of this information can be gleaned through the seemingly simple act of "liking" something. If you like a lot of Republicans politicians but no Democrats, then you are sending a message about your political affiliations.

A recent article published by the Wall Street Journal (link) revealed that Facebook intends to tailor advertisements that it will display onscreen during an active Facebook session by accessing web browser history information that is cached on the computer. That means that when a person is logged into Facebook that the Facebook web server(s) are scanning that person's machine for data to boost its advertising revenue….

To read more click HERE

GCHQ Has the Permission to Intercept Facebook, Google, Twitter Communications
SoftPedia, 17 Jun 2014: The GCHQ, the British intelligence agency, has revealed a secret government policy that justifies the mass surveillance of UK users of Facebook, Twitter, YouTube and Google. Charles Farr, the director general of security and counter terrorism, has issued a witness statement in which he explained how the law actually permitted intercepting tweets, Google and YouTube searches, as well as Facebook posts, as these communications were classified as "external communications." The Regulation and Investigatory Powers Act (RIPA) allows authorities to indiscriminately listen to or search through these types of communications. For better clarification, these are those messages that are sent and received outside the British Islands, regardless of whether they passed through the area or not. For example, Facebook has data centers in the United States and in Sweden, which means that they're "outside the British Islands." This means that any Facebook status update has to communicate with one of these data centers before returning, effectively leaving the UK. RIPA allows all this data to be looked into regardless of whether there are reasons to suspect the owner of wrongdoing or not. Agents cannot look through the content by using keywords or terms that mention someone living in the United Kingdom. The UK uses the threat of terrorism to justify the permission for such a blatant invasion of people's privacy. Furthermore, Farr states that sharing the communications data from foreign intelligence partners, especially from the United States, has helped prevent terrorist attacks and serious crimes, something that the NSA has been saying for a year, but which has never been proven. As a matter of fact, in the case of the NSA, several groups that looked into the agency's activities have failed to come up with a solid example where the collected data has helped prevent a terrorist attack. Last month, the GCHQ was slapped with a legal complaint by several privacy activists groups after reports that the agency was using its hacking tools to infect computer and smartphones alike with malicious software. This allowed them to remotely hijack the user's camera, as well as their microphones. The GCHQ's actions have come up on several occasions in the leaked documents of Edward Snowden. More specifically, the agency's strong tie with the NSA has been exposed. Recently, it has been revealed that the GCHQ and the NSA use malware to conduct surveillance that has the potential of being far more intrusive than any other program exposed so far. To read more click HERE

Customer Details Stored in Plain Text - Stratfor Hack Forensic Report
SoftPedia, 17 Jun 2014: A recently leaked report of the Verizon forensic investigation on the AntiSec breach of Stratfor (Strategic Forecasting, Inc.) systems back in 2011 showed that prior to the attack the company suffered from a massive lack of security. Finished on February 15, 2012, the investigation revealed that the first signs of unauthorized access were recorded on September 29, more than a month before the breach. There were numerous causes that allowed the intrusion to happen, the absence of file integrity monitoring instruments being at the head of the list, because this permitted the attacker(s) to insert custom scripts and execute them undetected. The report notes that all the affected systems (web server, database server, mail server, Active Directory server) could be accessed remotely on a permanent basis, without the possibility to verify or log the sessions. Access could be done either via SSH (Linux) or Windows Remote Desktop, and no restriction was enabled based on IP addresses or geolocation of the

user. According to the document, the back-end database for the e-commerce process of the company included Primary Account Number (PAN), expiry date and CVV2/CVC2 values, all of them stored in plain text. Another security measure that was not available for the sensitive systems was a firewall, whose purpose would have been to filter the traffic or block it along with accompanying data. As a result, information on the e-commerce network could be exchanged unrestrictedly. The forensics document notes that "systems interacting with the cardholder data were directly accessible from the systems within the corporate subnet with single-factor authentication." Separating server systems with various functionalities is a paramount security measure that guarantees network protection from various forms of exploitation. Keeping the network segments separated by imposing communication restrictions between them is specifically designed to prevent an attack on one system to expand to the other parts of the network, thus minimizing the damage. Furthermore, the leaked file points out that Stratfor did not maintain centralized logging to monitor on a frequent basis for suspicious activity or out of the ordinary security events. Given the conclusions of the report, the attacker(s) benefited from a lot of help from the company. It appears that there was no password management policy in place either, since the same countersigns were sometimes used by several employees on multiple devices, which allowed targeted attacks designed to obtain the credentials. Oftentimes, the same password was used by employees for accessing both the email and remote systems containing sensitive information. On December 24, 2011, AntiSec group defaced Stratfor website and initiated the deletion routine using the "rm-rf" Unix command on the root directory with elevated privileges, causing the server to crash when critical systems were removed. A day later, on December 25, some of the information taken from Stratfor was dumped online. The data exfiltrated during the breach contained customer names, email addresses, primary account numbers, expiration date of the cards and CVV2/CVC2 values. A tweet from Anonymous on December 26, 2011, informed that the attacker(s) stole 860,000 usernames, 75,000 credit card details and more than 2.5 million company emails. STRATFOR details: 860,000 usernames; 75,000 credit card data; +2.5 million Stratfor emails; 4 servers rooted/wiped | http://t.co/eVHSCuzn — Anonymous (@YourAnonNews) To read more click HERE

Simplelocker Gets Decrypted

SoftPedia, 17 Jun 2014: Simon Bell, the UK student that presented an in-depth analysis of the Simplocker code, has just released the solution for decrypting the files taken hostage by the ransomware. It relies on using the built-in decrypt method and the password mentioned in the initial post. "This means we're able to create our own Java class and copy the decryption code from the ransomware into our antidote class," writes Bell. After creating a new Java class with the methods for targeting the encrypted data and for setting the decryption password, Bell integrated the constructor method in order to get the job done. The compiled result should be able to look for the locked items and run the decryption routine on them. The student also provides an alternative for overriding the default cipher password. The new post details all the steps necessary to build a Java application that can scan for the encrypted data and try to unlock it using the predefined password (link). Getting to a successful result in this case was an easy job, but since Simplocker is considered more of a proof-of-concept than a real threat, future malware derived from it will feature code obfuscation and protection methods to prevent detection and analysis. To read more click HERE

Evernote's Forum Server Has Been Hacked

SoftPedia, 17 Jun 2014: The security of the discussion forum server for Evernote has been breached, and it appears that the hacker(s) managed to get access to the profile information of some members. The company sent an email to the affected users explaining the current situation and asking them to change their passwords if they are used to log into other web services as well. In a post on the forum, Geoffrey Barry, Community Manager at Evernote, said that the discussion site is a separate service from the note-taking one and that all other content is safe and sound. Since the forum and the note-taking function on different networks, which are not connected to each other, the company representative made it clear that the log-in password for Evernote does not have to be modified. "We do not store your Evernote password on our discussion forum servers and you do not need to change it," the post said. According to Barry, users with an older account on the forum, created in 2011 or earlier, are the ones affected by the breach and should update the countersign. All passwords are protected by a hashing algorithm, which should make the hackers' job to determine the string more difficult. Additional information leaked during the attack includes email addresses and, if provided, birthday details. In 2011, Evernote introduced the single-sign-on service, which means that the same password used to log into the service is also used for the forum. However, the information for the forum accounts created after 2011 should be safe because they are stored on Evernote's servers, whose security has not been breached. This created confusion among users reading the post announcing the hack because they immediately proceeded towards changing the log-in password and were directed to the Evernote account. To clear things up, Barry made another post on the forum, saying that "Evernote passwords have NOT been compromised. The only passwords that were compromised as part of this breach would be to forum accounts (which had their own passwords) created on the old forum system, which is no longer active. Since 2011 the forum authenticates you via a Single Sign On with your Evernote account, which allows you to log into our forums by logging into your Evernote account." Furthermore, the representative added that, "The only scenario where you would need to change your Evernote account password is if you used the same password on forum.evernote.com (the site that predates discussion.evernote.com forums in 2011) as your Evernote account password, and have not made any changes to your passwords since." The bottom line is that only users that received the email informing of the risk need to update their passwords. Last week, Evernote was hit by a DDos attack, which was resolved quickly by the company. To read more click HERE

Internet Explorer Script Engine Susceptible to Attacks

Softpedia, 16 Jun 2014: Exploit mitigation techniques available in Internet Explorer keep the browser strong in face of memory exploits, but attacks could be carried out through the script interpreter engine. In a blog post from network security firm Fortinet security researcher Zhenhua Liu explains how exploit researchers may have opened the box of Pandora as far as the safety of Microsoft' browser is concerned. He shows that scripts can be as efficient as a shellcode and that malicious scripts can be run by script interpreter engine on a target machine with escalated privileges, based on the discoveries of Yang Yu (CanSecWest 2014 presentation), Yuki Chen and Yuange (Chinese). Liu says that "the safety of the IE script engine relies solely on one single byte - the SafetyOption flag." Getting elevated privileges requires modifying the flag to 0 (zero) or in JScript and 0 (zero) in VBScript. The COleScript::CanCreateObject and ColeScript::CanObjectRun are the functions that perform separate checks on the SafetyOption flag to decide if it is safe to create and run a given ActiveX object. Penetrating the protection layers is not that simple, though. For the trick to work, the attacker needs to know the memory address of the flag, hence full process memory access is required, which is not actually impossible (zero-day vulnerabilities still continue to pop up). On the other hand, if full process memory access has been gained, the attacker can modify the SafetyOption flag and execute malicious scripts with elevated privilege. The researcher warns that the exploit model works with Internet Explorer 11, too, but the flag can only be modified in VBScript because the protection for the JScript engine has been strengthened by introducing a 0x20-byte hash value. As such, when "the SafetyOption flag is used, the function ScriptEngine::GetSafetyOptions is called to generate a new hash that is then compared with the original hash value, which is stored in memory." However, it appears that the two functions checking the flag for permission are still responsible for enabling elevated privileges and even if SafetyOption returns a non-zero value, the action can be completed by modifying the application data in the ScriptEngine object. The researcher predicts more zero-day vulnerabilities to appear, "Since the only prerequisite for using this is a vulnerability for an arbitrary write (which is common nowadays), we can anticipate more zero-days that will use this technique in the near future." He applauds the fact that in edge mode, Internet Explorer 11 does not support VBScript and suggests better security of the JScript engine (referring to the member data in the object and disabling some privileged methods), along with "implementing randomization in the IE custom heap management." To read more click HERE