THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

13 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 10, Securityweek – (International) **New Zeus variant targeting online banking users in Canada.** Security researchers at Trusteer identified a new variant of the Zeus banking trojan known as Zeus.Maple that has been in use since January 2014 and is primarily targeting major Canadian financial institutions. The variant improves on features from past versions but does not add new functionality. Source: http://www.securityweek.com/new-zeus-variant-targeting-online-banking-users-canada

June 10, Associated Press – (International) **Nigerian man admits role in computer fraud scheme.** A Nigerian man pleaded guilty June 10 in New Jersey for his role in an identity theft scheme that defrauded vendors out of nearly $1 million in office supplies. The scheme involved phishing attacks which mimicked Web pages of U.S. government agencies and legitimate emails, causing agency employees to visit fake sites and provide their credentials, allowing orders of office supplies that were received overseas. Source: http://www.sfgate.com/news/article/Nigerian-man-admits-role-in-computer-fraud-scheme-5542545.php

June 11, The Register – (International) **Feedly DDoSed by ransom-threat crims: 'We refused to give in.'** News aggregator service Feedly was knocked offline June 11 by a distributed denial of service (DDoS) attack after the company refused to pay attackers a ransom to stop the attack. Other entities were targeted by the same group, with Evernote reporting being knocked offline for a time by another DDoS attack. Source: http://www.theregister.co.uk/2014/06/11/feedly_ddos_ransom_attack

June 10, Threatpost – (International) **Microsoft patches IE8 zero day, critical Word bug.** Microsoft released its June round of Patch Tuesday updates, with a total of seven updates. Included was a patch for a zero day vulnerability in Internet Explorer 8, as well as a vulnerability in Word 2007. Source: http://threatpost.com/microsoft-patches-ie8-zero-day-critical-word-bug

June 10, SC Magazine – (International) **Online gambling site hit by five-vector DDoS attack peaking at 100Gbps.** Incapsula reported that it responded to a distributed denial of service (DDoS) attack on a customer's online gambling Web site June 6 that used five different vectors to create a 100 gigabits per second attack. Source: http://www.scmagazine.com/online-gambling-site-hit-by-five-vector-ddos-attack-peaking-at-100gbps/article/355020/

June 10, Dark Reading – (International) **Zeus being used in DDoS, attacks on cloud providers.** Researchers with the Prolexic Security Engineering and Response Team released a threat advisory that describes how the Zeus trojan and toolkit is being equipped with new payloads to perform attacks outside its usual use in banking fraud. Zeus was identified being used in a variety of attacks including distributed denial of service (DDoS), spam, virtual currency mining, and attacks on platform as a service (PaaS) and software as a service (SaaS) infrastructure. Source: http://www.darkreading.com/zeus-being-used-in-ddos-attacks-on-cloud-providers/d/d-id/1269554

June 12, The Register – (International) **Sealed with an XSS: I gave TweetDeck a heart attack, says teen comp sci boff Firo.** A computer science student who identified a basic cross-site scripting (XSS) flaw in Twitter's TweetDeck client stated that the vulnerability was spotted while experimenting with the HTML heart-symbol character. The vulnerability caused Twitter to shut down the TweetDeck client for some users due to others abusing the XSS vulnerability. Source: http://www.theregister.co.uk/2014/06/12/tweetdeck_xss_vuln_uncovered_by_heart_hunting_teenager/

June 11, Securityweek – (International) **Twitter fixes TweetDeck XSS security vulnerability.** Twitter disabled its TweetDeck app for about an hour June 11 after a cross-site scripting (XSS) vulnerability was discovered that could allow XSS to be executed by viewing a specially-crafted tweet. Researchers at Rapid7 reported that the issue primarily affected users of the TweetDeck plugin for Chrome. Source: http://www.securityweek.com/twitter-fixes-tweetdeck-xss-security-vulnerability

June 11, Securityweek – (International) **Chrome, Firefox updates address security vulnerabilities.** Google released an update for its Chrome browser, closing four security vulnerabilities. Mozilla also released an update for its Firefox browser, which closed seven vulnerabilities, five of which were rated as critical. Source: http://www.securityweek.com/chrome-firefox-updates-address-security-vulnerabilities

June 11, Securityweek – (International) **Adobe issues security updates for Flash Player, AIR.** Adobe released updates for several versions of its Flash Player and AIR products June 10, including updates for Flash Player for Windows and Mac OS X which were rated as high priority due to current or potential attacks exploiting those vulnerabilities. Source: http://www.securityweek.com/adobe-issues-security-updates-flash-player-air

OpenSSL Regression Found and Closed by Canonical in Ubuntu

SoftPedia, 13 Jun 2014: Details about an OpenSSL regression in Ubuntu 14.04 LTS, Ubuntu 13.10, Ubuntu 12.04 LTS, and Ubuntu 10.04 LTS operating systems have been published by Canonical in a security notice. A few days after Ubuntu developers integrated quite a few OpenSSL fixes for some recent problems that had been identified in the cryptographic library, the devs had to push another update to correct a regression. According to the security notice, "USN-2232-1 fixed vulnerabilities in OpenSSL. The upstream fix for CVE-2014-0224 caused a regression for certain applications that use tls_session_secret_cb, such as wpa_supplicant. This update fixes the problem." The initial vulnerability stated that, among other issues, OpenSSL incorrectly handled invalid DTLS fragments and remote attackers could have used this issue to cause OpenSSL to crash, resulting in a denial of service. This is just one of the issues fixed by the previous update, but only one regression was registered. The issue can be fixed if you upgrade your system(s) to the libssl1.0.0 specific to each distribution. To apply the patch, you can simply run the Update Manager application and enter apt-get update and apt-get dist-upgrade from the terminal. In general, a standard system update will make all the necessary changes and you will have to reboot the system. To read more click HERE

Facebook Accounts Are Gold for Cybercrooks

SoftPedia, 13 Jun 2014: By taking a swing at a social network account and successfully hijacking it, a cybercriminal opens the door to plenty more potential victims. Facebook is the main target in such cases because it is so good a platform for sharing information, which allows bad actors to lure a lot of users. Malware, spam and phishing links directing users to pages serving carefully planted threats are easily distributed from a stolen Facebook account. As noted by Nadezhda Demidova, Web Content Analyst at Kaspersky Lab, criminals can use the account for financial gains, "such as extorting money from the hijacked account's friends. The fraudster can send messages asking people to send money for help." Other reasons are the collection of information for launching targeted phishing attacks and even selling the account to other criminals. Getting their hands on a social network account is done through various methods, ranging from fake notifications, emails sent from a compromised address of a friend and forum messages to banners on third-party resources. In all these cases, the victim can be attracted to phishing pages where they are asked to log into a fake social network; the details are then sent to the attacker. A compromised Facebook account can also be used to direct the friends of the owner to malicious pages. In the case of fake Facebook messages, one way to notice the phishing attempt is to check in the address bar if the connection is secure. A green lock is a sign that the page is genuine. However, in the case of mobile devices, the address bar can oftentimes be hidden after the page is opened in order to capitalize on the display area, bringing the user one step closer to becoming a victim. Information from Kaspersky Security Network shows that in 2013 the anti-phishing heuristic component was triggered by phishing sites imitating social network websites in more than 35% of the cases. On the same note, compared to other social networks, Facebook accounted for 21.89% of the phishing alarms, while competition recorded a little more than half of that, 13.50%. In the United States, as many as 7,500 incidents were recorded. Keeping a vigilant eye on the resources that are accessed is the best way to minimize the phishing risk. Alarm bells should be ringing when you are asked to enter Facebook credentials into other forms than the official login page, especially if the connection is not secure, or when being redirected to webpages after clicking on a banner promising juicy content. "If suspicious emails and/or notifications start coming from your friend(s), try to contact them: their email or social network account may have been compromised or hijacked. If so, your friend(s) will need to change the password immediately," notes Demidova. To read more click HERE

Cloud-Based POS Software Subject to Targeted Attacks

SoftPedia, 13 Jun 2014: In a recent report, Los Angeles-based security firm IntelCrawler has revealed that cloud-POS software is vulnerable to attacks that would allow malicious actors access to customer personal identification information. Cloud-POS software allows retail companies to synchronize POS (point-of-sale) information with a remote server. This allows merchants round the clock web-based access to the data from any device that has a web browser installed. Apart from being cost-efficient, the advantages of a cloud-based POS system consist in instant centralization of data along with the possibility to create data and have it synchronized across all POS devices in the network. According to IntelCrawler, a compromised cloud-based POS service permits modifications regarding gift card information. This can be anything from creating new gift cards to altering discount vouchers. Furthermore, once they gain access to the system, cybercriminals can penetrate employee management sub-systems, which can easily lead to internal fraud. Named POSCLOUD.Backdoor/Agent, the malicious software is equipped with spyware capabilities, which allow the criminals to steal customer information. Even if it cannot be used by them directly, there is an underground digital market for such details. The report notes that "the extracted PII is then sold to underground identity thieves and also used for cyber espionage against large number of customers from different countries." POSCLOUD.Backdoor/Agent has the capability to download and unpack different modules from the command and control server in order to expand its functionality. Features identified by the security company include interception of forms and credentials "and to detect if the compromised PC has network connection with specific cloud-based POS providers." Additionally, the bad actors are able to collect information even if the data is encrypted, thanks to keylogging functionality. In order to do so, the operator has to be working with the software. In a comment for SC Magazine, CEO of IntelCrawler, Andrew Komarov, says that the malware was identified after a pretty big botnet takedown and he believes it to have been developed in private circles specifically for targeting cloud-based environments in order to collect customer data, credit card information included. There is no solid information about the identity of the group behind POSCLOUD.Backdoor/Agent, but the company speculates that they are based within the limits of the European Union. IntelCrawler's Cyber Threat Intelligence Team has notified the parties they identified as compromised, which consist in retailers and small businesses, and contacted global law enforcement organization, providing them a list with the infected IP addresses. To read more click HERE

Hacker Guccifer Indicted in the US

SoftPedia, 13 Jun 2014: 42-year-old Marcel Lehel Lazar, better known as Guccifer, the hacker that gained unauthorized access to email and social network accounts of high-profile public figures, has been charged in the United States. The indictment document, filed in U.S. District Court for the Eastern District of Virginia, specifies that Guccifer, who also acted under the aliases of "Guccifer Seven" and "Micul Fum," is indicted as follows:

- three counts of wire fraud;
- three counts of unauthorized access of a protected computer;
- one count of aggravated identity theft;
- one count of cyberstalking;
- one count of obstruction of justice.

The hacker is a taxi driver from Arad, Romania, and he has already been convicted in his own country and is to serve four years in prison. The charges brought to him in Romania included unauthorized access to email accounts of public figures, politician Corina Cretu and George Maior, the chief of the Romanian Intelligence Service (SRI). The United States indictment does not reveal the names of the victims, nor his methods to carry out the deeds. However, the document mentions that among the victims were a family member of two former U.S. presidents, a sanitation engineer, a former U.S. Cabinet member, a former member of the U.S. Joint Chiefs of Staff and a journalist and a former presidential advisor. Through methods unrevealed to the public, the document states that Guccifer obtained access to AOL, Facebook, Yahoo! and Gmail accounts. His actions included stealing content such as confidential information and property such as emails, images, medical information, phone numbers, home addresses or contact names. In some cases, he would change the original password to the accessed account. Some of the content stolen by the hacker has been leaked to media organizations, who published portions of the information in August, 2013. Among the alleged victims of the hacker there is former Secretary of State Colin Powell along with actors Leonardo DiCaprio, Nicole Kidman and Steve Martin. The U.S. Department of Justice also made available a press release informing of the allegations and that the case is being prosecuted by Trial Attorney Peter V. Roman of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Ryan K. Dickey of the Eastern District of Virginia. However, there is no information on when the trial will start and if Marcel Lehel Lazar is to be extradited after serving his sentence in Romania. To read more click HERE

Wi-Fi Spots and Malicious Chargers

SoftPedia, 12 Jun 2014: Security researchers point out the dangers of using a mobile device to connect to the Internet through unknown networks and the risk of charging them from untrusted places. Digital perils are even greater in Brazil, in the context of the 2014 World Cup championship, as cybercriminals spare no chance to lure in as many victims as possible. According to a study conducted in May in Sao Paolo by Kaspersky, security experts discovered more than 5,000 Wi-Fi access points while visiting various tourist attractions. Out of these, 5% had default SSID configuration, thus providing a potential attacker with extra information that could lead to finding a vulnerability and exploiting it to gain administrator access and control the data going through the network. Also, it is recommended to avoid connecting to ad-hoc networks because all the traffic is managed by a host that can be used to extract sensitive information. The study shows that a total of 26% of the networks analyzed by the research team were lacking any security measures. When using them, all the traffic is in plain text and even if the user accesses secure pages, not all websites have full SSL encryption, the risk of plain text information being still present. Attackers on the same network can intercept data and access it unrestrictedly. Man-in-the-middle (MitM) attacks are also possible, and cybercriminals can control the communication and impersonate the endpoint the victim tries to access. Researchers advise users to read the messages claiming that SSL certificates are out of date and to deny the connection. In order to maintain the safety of the data, users are recommended to rely on a VPN connection, which creates a tunnel between the local device and a secure server that routes the traffic to the intended destination. The traffic to the server is encrypted and safe from snooping. Another danger is the charging points. These can be tampered with and can leak information out of the phone during the battery charge through an USB port. Alternatively, the devices can be implanted with malware components with location tracking or information stealing capabilities; call records, messages, notes, pictures, contacts and documents can be extracted any time the device connects to the Internet. In this case, the recommendation goes for trying "to optimize battery life by shutting down unnecessary processes and entering flight safe mode when a cellphone network is not available. You can also disable sounds, vibrate tones and other resource-hungry features, like animated wallpapers etc." To read more click HERE