THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

3 November 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

October 29, IDG News Service – (International) **Cybercriminals create platform for automating rogue credit card charges.** Researchers with IntelCrawler reported that a Web-based application known as Voxis Platform that automates purchases from stolen payment card data has been sold on underweb markets since August. The application purports to use 32 different payment gateways and other methods to mimic normal card use and avoid detection. Source: http://www.networkworld.com/article/2840753/cybercriminals-create-platform-for-automating-rogue-credit-card-charges.html

October 29, Dark Reading – (National) **White House says unclassified network hit in cyberattack.** A White House National Security Council official confirmed October 29 that an unclassified portion of the White House network was the victim of an ongoing cyberattack, resulting in temporary system outages and loss of network connectivity for some users. Authorities worked to mitigate the threat and the attack did not cause any damage to White House computers or systems. Source: http://www.darkreading.com/attacks-breaches/white-house-says-unclassified-network-hit-in-cyberattack/d/d-id/1317060

October 30, The Register – (International) **Drupalocalypse! Devs say it's best to assume your CMS is owned.** The developers of the Drupal content management system (CMS) warned that Drupal Web sites that were not patched within 7 hours of the disclosure of a critical SQL injection vulnerability October 15 should be considered compromised due to the simplicity of the vulnerability and how quickly it was leveraged by attackers. The developers advised affected admins to restore their sites from backup since applying the patch would only close the vulnerability to future use, not remove any malware already in place. Source: http://www.theregister.co.uk/2014/10/30/drupal_sites_considered_hosed_if_sqli_hole_unclosed/

October 30, Securityweek – (International) **"AirHopper" malware uses radio signals to steal data from isolated computers.** Researchers at the Ben Gurion University created a proof-of-concept malware dubbed AirHopper that was used to demonstrate a data exfiltration attack against air gapped systems using radio signals produced by the target system's graphics card. The attack requires adding the malware to the target system and installing malicious code onto a nearby mobile device in order to set up the channel for transmitting the data sent from the target system. Source: http://www.securityweek.com/airhopper-malware-uses-radio-signals-steal-data-isolated-computers

October 29, Securityweek – (International) **ICS-CERT warns of ongoing attack campaign targeting industrial control systems.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory warning about an ongoing attack campaign targeting human machine interface (HMI) products used in industrial control systems including GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC products. The campaign uses a variant of the BlackEnergy malware and shares the same command and control infrastructure as the Sandworm campaign team. Source: http://www.securityweek.com/ics-cert-warns-ongoing-attack-campaign-targeting-industrial-control-systems

October 29, Securityweek – (International) **Microsoft releases Fix It tool to disable SSL 3.0 in IE to muzzle Poodle attack.** Microsoft released a Fix It tool that allows users to disable SSL 3.0 in all supported versions of Internet Explorer, closing the vulnerability used in the POODLE attack. The company also announced that it will disable SSL 3.0 and fallback to SSL 3.0 by default in its products in the months ahead. Source: http://www.securityweek.com/microsoft-releases-fix-it-tool-disable-ssl-30-ie-muzzle-poodle-attack

October 31, Softpedia – (National) **Capital One employee accesses customer info without authorization.** Capital One stated in a letter to affected customers that a former employee at the bank gained unauthorized access to an undisclosed amount of customer data that included names, account numbers, and Social Security numbers. The company has increased security measures and law enforcement agencies are investigating. Source: http://news.softpedia.com/news/Capital-One-Employee-Accesses-Customer-Info-without-Authorization-463624.shtml

October 30, BankInfoSecurity – (National) **Phishing attack leads to title firm breach.** Fidelity National Financial notified an unspecified number of customers that personal and financial information including payment card, driver's license, and Social Security numbers may have been compromised when attackers gained access to employees' email accounts via a phishing attack. The company stated that an investigation showed that the attackers' goal was to obtain information in order to redirect scheduled money transfers. Source: http://www.bankinfosecurity.com/phishing-attack-leads-to-bank-breach-a-7502

October 31, Softpedia – (International) **RIG Exploit Kit used in Drupal CMS exploit incidents.** RiskIQ researchers observed the RIG Exploit Kit being used in attacks that exploit a critical SQL injection vulnerability in the Drupal content management system (CMS) to redirect users to the exploit kit. The researchers found that all instances of the exploit kit are hosted on a machine at a Selectel datacenter in Russia. Source: http://news.softpedia.com/news/RIG-Exploit-Kit-Used-in-Drupal-CMS-Exploit-Incidents-463685.shtml

October 31, Securityweek – (International) **iOS app vulnerability exposed GroupMe accounts.** A researcher identified and reported a vulnerability in the GroupMe app for iOS that could have allowed an attacker to hijack the account of another user due to the sign-up process for new accounts lacking rate limiting or a security lockout mechanism on a phone number verification process. The issue was reported August 28 and patched September 17, and the researcher stated that there was no evidence it was exploited before being fixed. Source: http://www.securityweek.com/ios-app-vulnerability-exposed-groupme-accounts

October 31, Help Net Security – (International) **Android dialer hides, resists attempts to remove it.** Researchers with Dr. Web identified a malicious dialer for Android dubbed Android.Dialer.7.origin that places calls to a paid service at regular intervals after infecting devices disguised as an app. The malware attempts to hide itself by deleting its shortcut, disabling the device earpiece during calls, and removing evidence of the calls from the call and system logs. Source: http://www.net-security.org/malware_news.php?id=2903

October 30, The Register – (International) **Danish court finds Pirate Bay cofounder guilty of hacking CSC servers.** A court in Denmark found a cofounder of the Pirate Bay Web site guilty of working with an anonymous accomplice to compromise servers belonging to U.S. company CSC that contained data for European governments between February and August 2012. Source: http://www.theregister.co.uk/2014/10/30/danish_court_finds_pirate_bay_cofounder_guilty_of_hacking_csc_servers/

Over 227,000 New Malware Samples Emerged Daily in Q3 2014

Softpedia, 1 Nov 2014: Cybercriminals have taken the fast lane to thieving and plundering, creating more than 20 million fresh strains of malware in the third quarter of the year, which translates into a rate of 227,747 new samples per day. Most of these do not pose a risk for users with a reputable antivirus application guarding their computer, but the sheer number of malicious items being spilled in the wild on a daily basis is overwhelming. Researchers with Panda Security made a report for the latest quarter of the year and found that most of the threats recorded through their systems were Trojans, accounting for 78.08% of the total number of samples, which does not come as a surprise because this category of malware encompasses a multitude of threats, ranging from backdoors, rootkits, infostealers, malware dowloaders and droppers, to ransomware and spyware. Viruses and worms come in second and third place, accounting for 8.89% and 3.92%, respectively, according to a presentation from Technical Director of PandaLabs, Luis Corrons. As far as the infection rates are concerned, Trojans were responsible for most of them, while potentially unwanted programs (PUPs) came in second, with 14.55%. Infection distribution per country shows that China is in the lead with 49.83%, with Peru and Bolivia trailing behind. According to the report, Europe is the region with the smallest number of infections, nine of the countries in this area being in the top ten most secure, with Norway and Sweden in the first places. Japan is the only Asian country on this list. However, it is unclear the computer platforms these metrics were collected from, or the visibility the company has across other regions of the globe. Malware for mobile operating systems has recorded an avid development and has evolved both in number and malicious capabilities. According to the International Telecommunication Unit, there are about 2.3 billion smartphones in the world, making mobile operating systems ripe for cybercriminal activity. A report from Kaspersky released in October reveals that most mobile malware has been created for Android, and in the first half of the year their systems picked up 175,442 new unique malicious programs for this operating system alone. Banking Trojans are the top threat for mobile phones, and as most malware for these devices, they come disguised as a legitimate app or update. The top cause of infection on Android, which is the most targeted mobile OS, is allowing the device to install apps that come from third-party stores poorly curated by their owners. To read more click **HERE**

New SQL Injection Flaw Puts Sony PlayStation User Data at Risk

Softpedia, 3 Nov 2014: Details of Sony Playstation Network users could be at risk due to a blind SQL injection bug in the website, a penetration tester claims. 20-years-old Aria Akhavan from Austria says that he uncovered the flaw that could allow an attacker to obtain information from the customer database by using SQL queries. A blind SQL injection is more difficult to exploit than regular SQL injections are, because the data is not displayed on the web page directly. Instead, the page returns a generic error message and the attacker needs to ask true or false questions through SQL statements in order to retrieve the database information. Although this type of attack requires more time to be carried out, it can be sped up by using automated tools when the target and the vulnerability have been pinpointed. The security researcher said in an interview to Effect Hacking that Sony was contacted about the matter in the middle of October, but by the end of the month an answer was still to be received. Akhavan also said that, at the time of the interview, the flaw had not been fixed. It is unclear what kind of data could be gleaned from this security vulnerability, but usernames and password hashes may be the least data that could be extracted. The penetration tester started reporting website vulnerabilities this year, in July, and has already alerted companies such as eBay and Avast of glitches that could be exploited by third parties. However, Akhavan said that he'd been studying penetration testing techniques for about five years; he declined to share an earnings total as a result of responsible disclosure of the bugs to companies. Sony is a constant target for hackers, and in a recent incident, a group known as the Lizard Squad initiated a massive DDoS (distributed denial-of service) attack on the company's services, cutting off access to the online playing network in various regions of the world. DDoS attacks are not designed to steal information, although they can be used to distract from a different attack that has this purpose. Back in 2011, Sony fell victim to multiple attacks from hacker outfits of the time, Anonymous and LulzSec. The latter managed to retrieve customer information (passwords, email addresses, home addresses, dates of

birth, and Sony opt-in data associated with their accounts) of over one million users of SonyPictures.com, by leveraging a simple SQL injection vulnerability. A previous attack on PlayStation Network, however, led to the compromise of personal and financial records of at least 77 million customers. To read more click **HERE**