THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

3 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

May 29, KTVX 4 Salt Lake City - (Utah) **America First Credit Union finds a breach in accounts that affects thousands.** America First Credit Union in Utah canceled debit card PINs and reissued debit cards starting May 29 for around 20,000 customers after it became aware of a data breach that occurred between October 2013 and February 2014. Source: http://www.good4utah.com/story/d/story/america-first-credit-union-finds-a-breach-in-accou/50239/gdD6BQR9hUmGyHqjfMcQBw

May 29, Threatpost - (International) **Iranian campaign snooped on U.S. officials.** iSight Partners researchers released a report stating that attackers from Iran created and ran a sophisticated cyberespionage campaign since at least 2011 targeting government officials, diplomats, U.S. military members, and Washington, D.C. journalists by creating fake online personas as reporters, defense contractors, and politicians. The attackers were allegedly able to access systems and gather information as well as email and network logins. Source: http://threatpost.com/iranian-campaign-snooped-on-u-s-officials

May 30, IDG News Service - (International) **New attack methods can 'brick' systems, defeat Secure Boot, researchers say.** A security researcher at Mitre demonstrated at the Hack in the Box 2014 conference that the Unified Extensible Firmware Interface (UEFI)'s Secure Boot mechanism can be bypassed on around half of computers in order to install bootkits. The researcher also demonstrated that a specific UEFI variable could be modified directly from the computer's operating system to make the system unusable. Source: http://www.computerworld.com/s/article/9248699/New_attack_methods_can_39_brick_39_systems_defeat_Secure_Boot_researchers_say

May 30, Help Net Security - (International) **Malware creation breaks all records! 160,000 new samples every day.** Panda Security reported that new malware creation occurred at record rates during the first quarter (Q1) of the year, with more than 15 million new samples observed during Q1. The researchers found that trojans made up 71.85 percent of new samples, and that some of the largest data thefts ever occurred during Q1, among other findings. Source: http://www.net-security.org/malware_news.php?id=2776

June 2, Threatpost - (International) **FBI, European authorities go after GameOver Zeus botnet.** U.S. and European law enforcement authorities and several companies cooperatively seized servers and disrupted the operations of the GameOver Zeus botnet May 30, and are seeking a Russian citizen allegedly connected to the operation of the peer-to-peer (P2P) botnet. The botnet is used to perform wire fraud by stealing financial credentials and then transferring money to accounts controlled by its operators. Source: http://threatpost.com/fbi-european-authorities-go-after-gameover-zeus-botnet

May 30, Threatpost - (International) **Apache patches DoS, information disclosure bugs in Tomcat.** The Apache Software Foundation released a patch for Tomcat, closing three information disclosure vulnerabilities and one denial of service issue. Users were advised to apply the patches to their installations. Source: http://threatpost.com/apache-patches-dos-information-disclosure-bugs-in-tomcat

June 2, Security Week - (International) **Middle East hackers target government departments, U.S. financial institution.** FireEye researchers identified an attack campaign targeting an undisclosed U.S. financial institution as well as government agencies in several countries that attempts to drop remote access trojans (RATs) on targets' systems. The researchers attributed the campaign to a Middle Eastern group known as "Operation Molerats" due to the location of the attack infrastructure and the variants of the Poison Ivy and Xtreme RATs used. Source: http://www.securityweek.com/middle-east-hackers-target-government-departments-us-financial-institution

May 30, Arkansas Business – (Arkansas) **Arkansas State notified of data breach; up to 50,000 could be affected.** Arkansas State University was notified by the Arkansas Department of Human Services May 28 that a database used by the College of Education and Behavioral Science's Department of Childhood Services was breached, potentially exposing the personal information of about 50,000 individuals. The third-party site was taken offline and authorities are investigating the incident. Source: http://www.arkansasbusiness.com/article/99018/arkansas-state-notified-of-data-breach-up-to-50000-could-be-affected

June 2, Security Week – (International) **New Heartbleed attack vectors impact enterprise wireless, Android devices.** A security researcher detailed new attack methods for using the Heartbleed vulnerability in OpenSSL which could allow attacks over the Extensible Authentication Protocol (EAP) used in wireless networks and peer-to-peer (P2P) connections. The new vectors can threaten enterprise wireless networks, Android devices, and other connections. Source: http://www.securityweek.com/new-heartbleed-attack-vectors-impact-enterprise-wireless-android-devices

June 2, The Register – (International) **Flaws open gates to WordPress en-masse SEO beat-down.** A patch was released June 1 for the popular All in One SEO Pack plugin for WordPress, closing vulnerabilities which could allow attackers to launch privilege escalation and cross-site scripting (XSS) attacks in sites using older versions of the plugin. Users were advised to update their installations. Source: http://www.theregister.co.uk/2014/06/02/flaws_open_gates_to_wordpress_enmasse_seo_beatdown/

Windows Users Given 2 Weeks to Get Malware off Their Computers

SoftPedia, 3 Jun 2014: Microsoft, the FBI, and some other companies across the world have recently managed to take down the central servers of the GameOver Zeus botnet, which has until now infected millions of computers with malware designed to steal bank details from affected PCs. Although Redmond itself guaranteed that it would help users who got their machines infected with the malware, Rik Ferguson, security researcher at Trend Micro, said that those who want to remove the malware from their computers have a maximum of two weeks to do so because the botnet could go back online very soon. "The ultimate goal of the law enforcement activity is to prevent infected computers from communicating with one another, significantly weakening the criminal infrastructure. While this blow is effective, it is not permanent and we expect the malicious networks to return to their former strength within weeks, if not days," he said. Victims and those who think that their computers got infected with Zeus malware only need to follow a few simple steps, he added, but they need to do it as soon as possible while the botnet is still down. As a result, when it's restored, the botnet won't have the same strength as before and you're going to be completely secure. First of all, download up-to-date anti-virus production that can detect Zeus malware and scan your computer to make sure that your computer is clean. Then, install all available patches for Windows, meaning that if you're still running Windows XP, you might be vulnerable to attacks. Third-party security software with real-time protection is also needed, Ferguson explained, in order to block future attacks and thus keep the malware away from your computer. Last but not least, you should help those around you do the same thing in order to block the botnet from expanding once again. The US-CERT is also warning users that running anti-malware software is a must these days, especially in case you suspect that GameOver Zeus malware has reached your computer. "GOZ, which is often propagated through spam and phishing messages, is primarily used by cybercriminals to harvest banking information, such as login credentials, from a victim's computer. Infected systems can also be used to engage in other malicious activities, such as sending spam or participating in distributed denial-of-service (DDoS) attacks," the US-CERT warned. To read more click **HERE**

Free DHS Cyber Assessments

ISSSource, 2 Jun 2014: Cyber attacks are growing and most people cannot deny that, but for the small- to medium-sized manufacturers, the idea of taking on a cyber security program can be daunting. That is why the Department of Homeland Security's (DHS) Office of Cybersecurity & Communications (CS&C) will conduct complimentary and voluntary assessments to evaluate operational resilience and cyber security capabilities within critical infrastructure sectors, as well as state, local, tribal, and territorial governments. The Cyber Security Evaluation Program (CSEP) administers the Cyber Resilience Review (CRR) while the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) offers the Cyber Security Evaluation Tool (CSET) for industrial control systems. Click **here** for more information on the program. To read more click **HERE**

Cyber Attack 'To Hit in Next Two Weeks'

Sky News, 2 Jun 2014: Computer users are being urged to protect their machines from malware which could allow hackers to steal financial data. British investigators have been working with the FBI to trace the hackers behind an attack, which they expect to take place in the next fortnight. Between 500,000 and one million machines have so far been infected worldwide, according to court documents. US officials have accused a Russian hacker of masterminding the scam - and prosecutors say those involved have already raked in more than $100m (£60m). The National Crime Agency (NCA) is now warning of a "powerful computer attack". It is urging people to back up important files and make sure their security software and operating system are up to date. Two pieces of malware software known as GOZeuS and CryptoLocker are responsible for the alert. They typically infect a computer via attachments or links in emails. If a user clicks on GOZeuS, it silently monitors activity and tries to capture information such as bank details. "(The links or attachments) may look like they have been sent by genuine contacts and may purport to carry invoices, voicemail messages, or any file made to look innocuous," the NCA warned. "These emails are generated by other victims' computers, who do not realise they are infected, and are used to send mass emails creating more victims." The Cryptolocker malware is activated if the first attack is not profitable enough. It locks a user from their files and threatens to delete them unless a "ransom" of several hundred pounds is paid. Some 234,000 machines were hit by Cryptolocker - bringing in $27m (£16m) in payments - in its first two months, the US Justice Department said. More than 15,500 computers in the UK are infected and "many more" are at risk, according to the NCA. Stewart Garrick, a senior investigator with the NCA, told Sky News the threat was mainly against individuals or businesses running Windows-based computers. Thirty-year-old Russian Evgeniy Bogachev is the alleged leader of the gang behind the attacks, FBI executive assistant director Robert Anderson told a news conference in Washington DC. US and other agents seized servers around the world this weekend and freed 300,000 computers from the infection. "They (the FBI) have disrupted the network and taken control of it," said Sky's Tom Cheshire. To read more click HERE