Counterintelligence Working Group NEW MEXICO

NMCIWG Purple Arrow

The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
3 April 2014

Purpose
Educate recipients of cyber events to aid in the protection of electronically stored corporate proprietary, DoD and/or Personally Identifiable Information from theft, compromise, espionage, and / or insider threat

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

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, Sandia Labs

April 1, Topeka Capital-Journal – (Kansas) **Cyber attacks paralyze state math and reading tests.** The Kansas Department of Education confirmed April 1 that attackers began using distributed denial of service (DDoS) attacks March 27 targeting the State's testing platform operated by the University of Kansas' Center for Educational Testing and Evaluation in order to hinder annual math and reading tests. Testing was temporarily put on hold while authorities worked to mitigate another DDoS attack. Source: http://cjonline.com/news/2014-04-01/cyber-attacks-paralyze-state-math-and-reading-tests

April 2, Help Net Security – (International) **Passwords, messages of 158k+ Boxee.tv users leaked.** Attackers compromised the forum database for Web TV service Boxee.tv and posted the private information for over 158,000 users. The breach and subsequent leak contain email addresses, encrypted passwords, dates of birth, message histories, IP addresses, and other information. Source: http://www.net-security.org/secworld.php?id=16621

April 2, Softpedia – (International) **Cybercriminals abuse security camera recorders and routers to mine for Bitcoins.** A researcher at the SANS Technology Institute identified malware designed to infect security camera recorders and routers and use the devices to attempt to mine Bitcoin virtual currency. The malware is designed to run on ARM infrastructure and was spotted on Hikvision DVRs, which have a simple default root password that users often do not change. Source: http://news.softpedia.com/news/Cybercriminals-Abuse-Security-Camera-Recorders-and-Routers-to-Mine-for-Bitcoins-435427.shtml

April 2, Help Net Security – (International) **Apple releases Safari 7.0.3, fixes security.** Apple released version 7.0.3 of its Safari browser, fixing several security issues and adding compatibility and stability improvements. Source: http://www.net-security.org/secworld.php?id=16620

April 2, Softpedia – (International) **SellHack deactivates plugin after cease and desist letter from LinkedIn.** The makers of the SellHack browser plugin, which uses publicly visible data to help users obtain hidden email addresses of LinkedIn users, deactivated the plugin April 1 following a cease-and-desist letter from LinkedIn. Source: http://news.softpedia.com/news/SellHack-Deactivates-Plugin-After-Cease-and-Desist-Letter-from-LinkedIn-435315.shtml

April 2, Softpedia – (International) **Oculus VR finds SQL injection flaw, asks Developer Center users to change passwords.** Oculus VR advised users of its Oculus Developer Center to change their passwords as a precaution after the company identified a SQL injection vulnerability. The company reported that there was no indication that the vulnerability had been exploited. Source: http://news.softpedia.com/news/Oculus-VR-Finds-SQL-Injection-Flaw-Asks-Developer-Center-Users-to-Change-Passwords-435302.shtml

April 1, The Register – (International) **Password bug lets me see shoppers' credit cards in eBay ProStores, claims infosec bod.** A security researcher from Securatary disclosed March 20 that he identified a vulnerability in eBay's ProStores shops that could have allowed attackers to credit themselves with gift cards for ProStores and obtain customer payment card information. The vulnerability was reported in February and later fixed by eBay. Source: http://www.theregister.co.uk/2014/04/01/ebay_stores_vuln/

April 1, The Register – (International) **Hotmail-gate: Windows 8 code leaker pleads guilty to theft of trade secrets.** A former Microsoft employee pleaded guilty March 31 to stealing company trade secrets for sending unreleased updates for the RT operating system as well as a copy of the Microsoft Activation Server Software Development Kit to a blogger. Source: http://www.theregister.co.uk/2014/04/01/kibkalo_guilty_plea/

Federal agencies have dropped the ball on data breaches

GAO Reuters, 2 Apr 2014: Federal agencies have a spotty record of handling data breaches, which can include the theft of sensitive information such as Social Security numbers, financial data and health history, the investigative arm of the U.S. Congress said in a report on Wednesday. The number of such incidents involving personal data increased to 25,566 last year from 10,481 in 2009, the Government Accountability Office said. That total included both cyber crime and non-cyber breaches. Incidents have ranged from the highly publicized theft in 2006 of a laptop and external hard drive belonging to the Veterans Affairs Department that contained personal data on 26.5 million veterans and active duty members of the military, to the hacking of a Federal Aviation Administration computer that contained data on 45,000 agency employees and retirees. "It is critical that federal agencies take steps to secure the information that they collect, retain, and disseminate and that, when events such as data breaches occur, they respond swiftly and appropriately," Gregory Wilshusen, the GAO's director of information security issues, said in remarks prepared for a congressional hearing on data breaches on Wednesday. Of the seven agencies whose breaches were analyzed by the GAO, only the Internal Revenue Service consistently calculated how much personal information was at risk in the incidents, and only the IRS and the U.S. Army documented how many people may have been affected, the report said. Only the Army and the Securities and Exchange Commission notified the people whose data may have been exposed. None of the federal agencies consistently offered credit monitoring services to the affected individuals, the report added. At the hearing of the Senate Committee on Homeland Security and Governmental Affairs, Federal Trade Commission Chairwoman Edith Ramirez urged lawmakers to enact a "strong federal data security and breach notification" law. Senators Tom Carper, a Democrat from Delaware, and Roy Blunt, a Missouri Republican, introduced a breach notification measure in January aimed at creating a single standard. But consumer groups have warned that companies may be pressing for a federal standard in hopes that it would be weaker than many of the state laws. California requires a detailed disclosure to consumers "in the most expedient time possible and without unreasonable delay" when personal information, including emails with passwords, is "reasonably believed" to have been stolen. To read more click **HERE**