The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

31 January 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

January 29, Reuters – (National) **Target: Hackers attacked with stolen credentials.** Target Corp., reported January 29 that the attackers who perpetrated a massive breach of customer payment card data used stolen vendor credentials to access the company's systems. Source: http://news.msn.com/us/target-hackers-attacked-with-stolen-credentials

January 29, SC Magazine – (National) **Neiman Marcus hack involved two pieces of malware.** Neiman Marcus reported that two pieces of malware were used to compromise its systems in a recent data breach, with the first inserted before July 2013 which allowed the payment card scraping malware to be uploaded later in the year. Source: http://www.scmagazine.com//neiman-marcus-hack-involved-two-pieces-of-malware/article/331669/

January 30, Memphis Commercial Appeal – (Tennessee) **Memphis College of Art security guard charged with stealing computer equipment.** A Memphis College of Art security guard was accused of stealing $10,725 worth of computer equipment from the Midtown school after officials reported five pieces of equipment went missing January 14. Source: http://www.commercialappeal.com/news/2014/jan/30/memphis-college-of-art-security-guard-charged/

January 30, Softpedia – (International) **Remote code execution vulnerability impacts Wikipedia and other MediaWiki sites.** Researchers at Check Point identified a critical vulnerability affecting Web sites created with the MediaWiki platform that could be exploited for remote code execution. The MediaWiki Foundation issued a patch to close the vulnerability and advised users to update their installations. Source: http://news.softpedia.com/news/Remote-Code-Execution-Vulnerability-Impacts-Wikipedia-and-Other-MediaWiki-Sites-422079.shtml

January 30, The Register – (International) **Security 101 fail: 3G/4G modems expose control panels to hackers.** A researcher found that several 3G and 4G USB modems are vulnerable to cross-site request forgery (CSRF) attacks that could allow attackers to access the modem's control panel Web page and tamper with the device. The vulnerabilities could be exploited to send messages to premium-rate numbers and steal user credentials. Source: http://www.theregister.co.uk/2014/01/30/3gmodem_security_peril/

January 30, Softpedia – (International) **Barracuda Networks identifies rogue SignNow version in App Store.** Barracuda Labs researchers identified a rogue version of their SignNow app in Apple's App Store, and found that developers listed as GameStruct and Tektrify are uploading rogue versions of other apps as well. Source: http://news.softpedia.com/news/Barracuda-Networks-Identifies-Rogue-SignNow-Version-in-the-App-Store-422306.shtml

January 29, SC Magazine – (International) **Before shutdown, ransomware op spreading "Icepol" caused 42,000 U.S. infections.** Bitdefender and Romanian authorities analyzed servers seized in relation to the Icepol ransomware and found that the ransomware was installed around 42,400 times in the U.S. between May and September 2013. An estimated $32,000 was stolen from U.S. victims. Source: http://www.scmagazine.com//before-shutdown-ransomware-op-spreading-icepol-caused-42000-us-infections/article/331677/

January 29, Threatpost – (International) **High-volume DDoS attacks top operational threat to businesses, service providers.** Arbor Networks released its Worldwide Infrastructure Security Report and found that distributed denial of service (DDoS) attacks were the largest operational threat to service providers and enterprises, reaching unprecedented levels in 2013, among other findings. Source: http://threatpost.com/high-volume-ddos-attacks-top-operational-threat-to-businesses-service-providers/103933

Experts Find 28 Security Issues in Oracle's Java Cloud Service

SoftPedia, 31 Jan 2014: Security researchers from Security Explorations have been analyzing Oracle's Java Cloud Service. Based on their findings, experts have determined that Oracle hasn't done a proper security review of the platform before launching it. Adam Gowdiak, the CEO of Security Explorations, has revealed that they've identified a total of 28 issues. 16 of them can be leveraged to "completely break Java security sandbox of a target WebLogic server environment." "An attacker can further leverage this to gain access to application deployments of other users of Oracle Java Cloud service in the same regional data center," Gowdiak said. The expert has told Softpedia that some of these vulnerabilities are independent of each other, while others need to be combined in order to work. "The vulnerabilities were tested in two Oracle Java Cloud data centers (US1 and EMEA1 respectively). They were verified to be present in ver. 13.1 and 13.2 (most recent) of Oracle Java Cloud Software," Gowdiak explained in a mailed statement. The nature of the security holes identified by researchers shows that Oracle hasn't put too much effort into securing the Java Cloud Service. "They illustrate known and widely discussed security risks related to Java. They also expose weak understanding of Java security model and attack techniques by Oracle engineers," he said. Security Explorations has notified Oracle regarding their findings and provided the company with source and binary codes. Tools that illustrate the vulnerabilities and attack scenarios have also been sent. However, Gowdiak says they haven't received any feedback – Oracle hasn't yet confirmed receiving the report. "We hope the next time Larry Ellison is about to choose between boats and work, work is gonna win as obviously certain areas at Oracle need actual work, not the improvisation," he concluded. To read more click **HERE**

Tor-Based Malware ChewBacca Used to Steal Card Data from POS Systems

SoftPedia, 31 Jan 2014: BlackPOS and Dexter are not the only pieces of malware used by cybercriminals to steal payment card data from point-of-sale (POS) systems. RSA researchers have found that the recently discovered ChewBacca Trojan is also used for similar operations. ChewBacca's existence was first brought to light in December 2013 by Kaspersky researchers. The information-stealing Trojan wasn't being offered on public forums. It has attracted the attention of security experts because it uses the Tor network to hide its communications. RSA says that the malware has been used to log track 1 and track 2 data from infected POS systems since October 25. The company says that the Trojan has been leveraged in attacks against dozens of retailers. Most of them are based in the US, but some of them are in Russia, Canada and Australia. However, RSA's Will Gragido has told DarkReading that the malware doesn't appear to be tied to the Target, Neiman Marcus or Michaels hacks. He has revealed that the individuals behind the ChewBacca campaign are most likely from Ukraine. ChewBacca is not very sophisticated, yet it can be highly efficient when it comes to stealing payment card information from infected devices. In order to steal card data, the malware has a memory scanner component that's designed to target credit card processing systems. The scanner dumps a copy of the process' memory and analyzes it for magnetic stripe data, which it extracts and logs. "Retailers have a few choices

against these attackers," said RSA FirstWatch Senior Security Researcher Yotam Gottesman. "They can increase staffing levels and develop leading-edge capabilities to detect and stop attackers (comprehensive monitoring and incident response), or they can encrypt or tokenize data at the point of capture and ensure that it is not in plaintext view on their networks, thereby shifting the risk and burden of protection to the card issuers and their payment processors." To read more click **HERE**

11 California High School Students Expelled After Hacking Computers to Change Grades

Softpedia, 31 Jan 2014: In December 2013, we learned that a dozen students of the Corona del Mar High School in Newport Beach, California, were suspected of changing their grades and obtaining tests after hacking into the school's computers. The Newport-Mesa Unified School District Board of Education has decided to expel 11 students. A 28-year-old private tutor named Timothy Lance Lai is said to have shown the students how to use a keylogger. They connected the device to teachers' computers in an effort to steal their access passwords. The school district has decided to expel the students after analyzing the case for hours in a closed session. This is the toughest penalty allowed by the Education Code. So far, no charges have been filed against Lai and the students, but the police are still looking into the case. To read more click **HERE**

Israel's National Cyber Bureau Prepares Cyberattack Response Task Force

SoftPedia, 31 Jan 2014: Representatives of Israel's National Cyber Bureau have revealed the government's intention to launch a new task force whose goal will be to help consumers and businesses in dealing with cyberattacks. In an interview with Bloomberg, the head of the National Cyber Bureau, Rami Efrati, has explained that the new cyber emergency response teams will focus on various types of incidents. Individuals and companies targeted in cyberattacks can file a report and they will be assisted by experts who specialize in certain areas. For instance, if a company from the financial sector is targeted, a professional with knowledge of cyberattacks against this industry will offer assistance. In addition to providing assistance to victims, the new program will also facilitate sharing of information regarding cyber threats. The National Cyber Bureau was established two years ago in an effort to coordinate responses to cyberattacks launched against Israel's critical systems. To read more click **HERE**

Hackers hit Yahoo email accounts, steal passwords

Yahoo, 30 Jan 2014: Usernames and passwords of some of Yahoo's email customers have been stolen and used to gather personal information about people those Yahoo mail users have recently corresponded with, the company said Thursday. Yahoo didn't say how many accounts have been affected. Yahoo is the second-largest email service worldwide, after Google's Gmail, according to the research firm comScore. There are 273 million Yahoo mail accounts worldwide, including 81 million in the U.S. It's the latest in a string of security breaches that have allowed hackers to nab personal information using software that analysts say is ever more sophisticated. Up to 70 million customers of Target stores had their personal information and credit and debit card numbers compromised late last year, and Neiman Marcus was the victim of a similar breach in December. "It's an old trend, but it's much more exaggerated now because the programs the bad guys use are much more sophisticated now," says Avivah Litan, a security analyst at the technology research firm Gartner. "We're clearly under attack." Yahoo Inc. said in a blog post on its breach that "The information sought in the attack seems to be names and email addresses from the affected accounts' most recent sent emails." That could mean hackers were looking for additional email addresses to send spam or scam messages. By grabbing real names from those sent folders, hackers could try to make bogus messages appear more legitimate to recipients. "It's much more likely that I'd click on something from you if we email all the time," says Richard Mogull, analyst and CEO of Securois, a security research and advisory firm. The bigger danger: access to email accounts could lead to more serious breaches involving banking and shopping sites. That's because many people reuse passwords across many sites, and also because many sites use email to reset passwords. Hackers could try logging in to such a site with the Yahoo email address, for instance, and ask that a password reminder be sent by email. Litan said hackers

appear to be "trying to collect as much information as they can on people. Putting all this stuff together makes it easier to steal somebody's identity." Yahoo said the usernames and passwords weren't collected from its own systems, but from a third-party database. Because so many people use the same passwords across multiple sites, its possible hackers broke in to some service that lets people use email addresses as their usernames. The hackers could have grabbed passwords stored at that service, filtered out the accounts with Yahoo addresses and used that information to log in to Yahoo's mail systems, said Johannes Ullrich, dean of research at the SANS Institute, a group devoted to security research and education. The breach is the second mishap for Yahoo's mail service in two months. In December, the service suffered a multi-day outage that prompted Yahoo CEO Marissa Mayer to issue an apology. Yahoo said it is resetting passwords on affected accounts and has "implemented additional measures" to block further attacks. The company would not comment beyond the information in its blog post. To read more click **HERE**