The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

7 - 9 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

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, Sandia 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 open source data

January 4, Associated Press – (Massachusetts; New Hampshire) **Stolen medical data prompts $150K fine.** The Department of Health and Human Services' Office for Civil Rights reported that Adult & Pediatric Dermatology settled any potential violations of health and security rules by paying $150,000 after a 2011 theft of a computer flash drive. The flash drive, which contained 2,000 patient records, was stolen from a locked car at an employee's home in Lowell, Massachusetts, and has not been recovered. Source: http://www.metrowestdailynews.com/news/police_and_fire/x579268196/Stolen-medical-data-prompts-150K-fine

January 4, Associated Press – (Virginia) **Va. benefit cards turned off due to Target breach.** The Virginia Department of Social Services announced Xeros deactivated nearly 4,000 State-issued electronic benefit cards that were used at Target Corp. stores after a security breach was announced by the retailer in December 2013. Source: http://www.nbcwashington.com/news/local/Va-Benefit-Cards-Turned-Off-Due-to-Target-Breach-238714961.html

January 6, Softpedia – (International) **Yahoo hacked, 2.5 million European users possibly infected with malware.** Researchers at Fox-IT discovered an attack that compromised Yahoo's ad service in order to redirect European visitors to Yahoo to domains hosting the Magnitude exploit kit, affecting as many as 2.5 million users. The attack lasted around 4 days and used Java vulnerabilities to push various pieces of malware. Source: http://news.softpedia.com/news/Yahoo-Hacked-2-5-Million-European-Users-Possibly-Infected-with-Malware-413732.shtml

January 6, The Register – (International) **Steam and Origin gamers knocked offline by SEPARATE DDoS attacks.** Distributed denial of service (DDoS) attacks launched by a group calling itself DerpTrolling caused disruptions to Electronic Arts' Origin gaming service for about 24 hours and Valve's Steam gaming service for about 1 hour January 3. Source: http://www.theregister.co.uk/2014/01/06/online_gaming_ddos_spate/

January 4, Softpedia– (International) **Trojan targeting WoW accounts disguised as Curse client.** Blizzard warned players of its World of Warcraft online game that a trojan designed to hijack accounts has been spreading disguised as a Curse client hosted on fake Web pages. Source: http://news.softpedia.com/news/Trojan-Targeting-WoW-Accounts-Disguised-as-Curse-Client-413555.shtml

January 7, SC Magazine – (International) **Prison Locker virus threatens to flood market.** Researchers at Malware Must Die identified a new piece of ransomware being advertised on underweb marketplaces named Prison Locker that encrypts all files on a computer except system files and .exe files and demands a ransom. Symantec researchers reported that the ransomware may already be in the wild after they obtained a piece of ransomware that they suspect is Prison Locker. Source: http://www.scmagazineuk.com/prison-locker-virus-threatens-to-flood-market/article/328183/

January 7, Softpedia – (International) **Windows zero-day used in attack targeted at embassies from Middle Eastern capital.** Trend Micro identified a cyberespionage campaign that targeted several embassies in an undisclosed Middle Eastern capital which utilized a zero-day vulnerability in Microsoft Windows XP and Server 2003 that was disclosed in November 2013. Phishing emails attempted to exploit the vulnerability and install a backdoor onto embassies' systems. Source: http://news.softpedia.com/news/Windows-Zero-Day-Used-in-Attack-Targeted-at-Embassies-from-Middle-Eastern-Capital-414388.shtml

January 7, Softpedia – (International) **World Poker Tour Amateur Poker League admits being hacked.** Representative for the World Poker Tour Amateur Poker League (WPTAPL) confirmed that their systems were compromised the week of December 30, 2013 and clear text email addresses and passwords of over 175,000 users were leaked. Included in the leaked emails were some U.S. government email addresses from federal agencies. Source: http://news.softpedia.com/news/World-Poker-Tour-Amateur-Poker-League-Admits-Being-Hacked-414236.shtml

January 7, Softpedia – (International) **Google, Yahoo, Amazon and Twitter domains impacted by Tajikistan registrar hack.** A hacker compromised the systems of Tajikistan's domain registrar, changing the DNS records for the Tajikistan domains of Amazon, Google, Twitter, and Yahoo and redirecting visitors to a defacement page. Source: http://news.softpedia.com/news/Google-Yahoo-Amazon-and-Twitter-Domains-Impacted-by-Tajikistan-Registrar-Hack-414220.shtml

January 7, Softpedia – (International) **T-Mobile warns customers that hackers obtained their SSNs.** T-Mobile notified customers that attackers breached a server operated by one of the company's suppliers and obtained names, addresses, driver's license numbers, and Social Security numbers for an undisclosed amount of customers in November 2013. Source: http://news.softpedia.com/news/T-Mobile-Warns-Customers-That-Hackers-Obtained-Their-SSNs-414524.shtml

January 8, Help Net Security– (International) **New Zeus variant stymies malware analysis, has rootkit capabilities.** Researchers at Trend Micro identified a new variant of the Zeus banking trojan which can prevent the execution of analysis tools and also has rootkit capabilities and the ability to hide files, folders, processes, and registry keys it creates or uses. Source: http://www.net-security.org/malware_news.php?id=2669

January 7, Washington Post – (Virginia) **Loudoun schools' data accidentally breached.** The Loudoun County school system in Virginia notified parents and employees after learning of an accidental security breach of personal data left unprotected through a third party vendor, Risk Solutions International, in 2013. An employee working on the school district's emergency management Web site mistakenly removed some security features, leaving the data online without password protection. Source: http://www.washingtonpost.com/local/loudoun-schools-data-accidentally-breached/2014/01/07/9ee816ea-780b-11e3-af7f-13bf0e9965f6_story.html

January 7, Boston Globe – (Massachusetts) **BU employees' direct-deposit pay stolen through alleged Internet scam.** Boston University temporarily shut down its electronic payroll system after learning that the system was breached through a phishing scam where scammers allegedly stole monthly direct-deposit paychecks from 10 university employees in December 2013 by changing their username and password information after obtaining their log-in credentials. Another 68 employees had work-related accounts accessed by an outside device, but officials do not believe any sensitive information was retrieved. Source:

http://www.boston.com/yourcampus/news/boston_university/2014/01/bu_employee_direct_deposit_pay_stolen_through_alleged_internet_scam.html

January 8, Help Net Security – (International) **OpenSUSE forums defaced via unknown vBulletin 0-day.** A hacker exploited a vulnerability in vBulletin to deface the forums of the openSUSE Linux distribution and download a database containing the usernames and email addresses of around 80,000 users. Source: http://www.net-security.org/secworld.php?id=16177

January 8, Softpedia – (International) **Expert finds clickjacking flaw in Google and open redirect in Facebook.** A security researcher identified and reported an open URL redirect vulnerability in Facebook that could be used to redirect users to other sites and a clickjacking flaw in the Google Maps site that could have been exploited to alter a user’s Google+ profile and hijack their webcam. Both vulnerabilities were closed by Facebook and Google. Source: http://news.softpedia.com/news/Expert-Finds-Clickjacking-Flaw-in-Google-and-Open-Redirect-in-Facebook-Video-414803.shtml

January 8, Softpedia – (International) **DailyMotion serves fake AV in malvertising attack.** Invincea researchers found that the video sharing Web site DailyMotion had been serving fake antivirus malware via malicious advertisements. Source: http://news.softpedia.com/news/DailyMotion-Serves-FakeAV-in-Malvertising-Attack-Video-414893.shtml