The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
24 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 23, Softpedia – (International) **Mining pool "Give Me Coins" hacked, 10,000 Litecoins stolen.** The administrators of the Give Me Coins virtual currency mining pool stated that the service was compromised by attackers who stole around $230,000 worth of the Litecoin virtual currency. The attackers were believed to have used a SQL injection vulnerability to breach the service. Source: http://news.softpedia.com/news/Mining-Pool-Give-Me-Coins-Hacked-10-000-Litecoins-Stolen-419921.shtml

January 23, Baltimore Sun – (Maryland) **Howard schools recover from possible cyber attack.** Officials from the Howard County Public School System in Maryland are investigating a possible cyberattack that may have caused intermittent Internet outages at various schools that persisted over the course of a week in January. Source: http://www.baltimoresun.com/news/maryland/howard/ellicott-city/ph-ho-cf-hcpss-internet-0123-20140121,0,3898276.story

January 23, The Register – (International) **When ZOMBIES go shopping; 40m Target customer breach? That's NOTHING!** An analysis of 139 U.S. retailers between November 2013 and January 12 performed by BitSight found 1,035 instances of unique malware infections actively communicating with attackers, averaging 7.5 infections per company. The Neurevt trojan was the most common piece of malware found during the analysis, among other findings. Source: http://www.theregister.co.uk/2014/01/23/retail_malware_epidemic/

January 23, SC Magazine – (International) **Potentially major XSS/JavaScript flaw found in Office 365.** Researchers at Cogmotive identified a vulnerability in Microsoft Office 365 that could allow a user with an organization email to use a JavaScript code to gain full administrator permissions across the organization's Office 365 environment. The vulnerability was reported to Microsoft and patched. Source: http://www.scmagazineuk.com/potentially-major-xssjavascript-flaw-found-in-office-365/article/330685/

January 23, Softpedia – (International) **Experts spot third variant of Mac trojan used by governments in targeted attacks.** Researchers at Intego identified a new variant of the Crisis trojan that targets Mac OS X systems and has been used by governments in targeted cyberattacks. Source: http://news.softpedia.com/news/Experts-Spot-Third-Variant-of-Mac-Trojan-Used-by-Governments-in-Targeted-Attacks-419899.shtml

January 23, Help Net Security – (International) **Facebook awards $33,500 bounty for critical flaw.** Facebook awarded a security researcher $33,500 as part of its bug bounty program for disclosing an XML external entities (XXE) vulnerability that could be exploited to allow attackers to read arbitrary files on Facebook's servers. Source: http://www.net-security.org/secworld.php?id=16251

January 23, Threatpost – (International) **Chrome eavesdropping exploit published.** A researcher released exploit code for a vulnerability he reported in Google's Chrome browser that could allow a malicious Web site to use a computer's microphone to eavesdrop without the user being aware. Source: http://threatpost.com/chrome-eavesdropping-exploit-published/103798

January 22, Softpedia – (International) **World Economic Forum's website plagued by XSS and other security issues.** Researchers at High-Tech Bridge identified several security issues on the Web site of the World Economic Forum, including cross-site-scripting (XSS) vulnerabilities, an invalid SSL certificate, and a flaw that exposed the email addresses of individuals who had contacted the organization. Source: http://news.softpedia.com/news/World-Economic-Forum-s-Website-Plagued-by-XSS-and-Other-Security-Issues-419674.shtml

January 22, Threatpost – (International) **Small number of malicious TOR exit relays snooping on traffic.** Researchers reported in a paper that 25 exit relays in the The Onion Router (TOR) network were configured maliciously or in a way that could present a security issue. The malicious or misconfigured exit relays could allow man-in-the-middle attacks and traffic monitoring. Source: http://threatpost.com/small-number-of-malicious-tor-exit-relays-snooping-on-traffic/103771

FBI warns retailers to expect more credit card breaches

Reuters, 23 Jan 2014 - The FBI has warned U.S. retailers to prepare for more cyber attacks after discovering about 20 hacking cases in the past year that involved the same kind of malicious software used against Target Corp in the holiday shopping season. The U.S. Federal Bureau of Investigation distributed a confidential, three-page report to retail companies last week describing the risks posed by "memory-parsing" malware that infects point-of-sale (POS) systems, which include cash registers and credit-card swiping machines found in store checkout aisles. "We believe POS malware crime will continue to grow over the near term, despite law enforcement and security firms' actions to mitigate it," said the FBI report, seen by Reuters. "The accessibility of the malware on underground forums, the affordability of the software and the huge potential profits to be made from retail POS systems in the United States make this type of financially motivated cyber crime attractive to a wide range of actors," the FBI said. The report was dated January 17 and entitled "Recent Cyber Intrusion Events Directed Toward Retail Firms." A spokeswoman for the FBI confirmed the agency had issued the report as part of efforts to share information about threats with the private sector. Retail, credit card and bank industry executives have become increasingly concerned about the security of payment card networks after Target, the No. 3 U.S. retailer, last month disclosed one of the biggest retail cyber attacks in history. The attack ran undetected for 19 days during the busy holiday shopping season and resulted in the theft of about 40 million credit and debit card records. The personal information of 70 million customers was also compromised. Luxury retail chain Neiman Marcus has said it too was the victim of a cyber attack, and sources have told Reuters that other retail chains have also been breached. Neiman Marcus said about 1.1 million customer cards were exposed by a data breach from July 16 to October 30 last year. In all these attacks, cyber criminals used memory-parsing software, also known as a "RAM scraper." When a customer swipes a credit or debit card, the POS terminal grabs the transaction data from the magnetic stripe and transfers it to the retailer's payment processing provider. While the data is encrypted during the process, RAM scrapers extract the information while it is in the computer's live memory, where it very briefly appears in plain text. RAM scraping technology has been around for a long time, but its use has increased in recent years. Developers of the malware have also enhanced its features to make it more difficult to be detected by anti-virus software deployed on POS systems running Windows software. The FBI said in its report that one variant of the malicious POS software, known as Alina, included an option that allowed remote upgrades, making it tougher for corporate security teams to identify and eradicate it. The report said at least one type of malware has been offered for sale for as much as $6,000 in a "well-known" underground forum. "The high dollar value gained from some of these compromises can encourage intruders to develop high sophistication methodologies, as well as incorporate mechanisms for the actors to remain undetected," the report said. Asked to comment on the FBI warning, the National Retail Federation industry trade group said retailers are alert to cyber risks. "Retailers have been and remain vigilant in their efforts to provide the highest level of security for their data systems in order to protect against malicious and criminal acts," NRF Vice President Tom Litchford said in a statement. "As the criminal investigation continues and more information becomes available, you can be sure that the retail industry will be responsive and engaged to ensure this particular cyber-attack does not happen again." One cyber security consultant who has reviewed the FBI report, said the findings were troubling. "Everybody we work with in the retail space is scared to death because they don't have a lot of defenses to prepare against these types of attacks," said the consultant, who is advising several retailers in current investigations. "This is not just based on anybody saying 'This is going to happen.' This is based on statistical data that the FBI is seeing," said the consultant, who was not authorized to publicly comment on the details of the report. Retailers need to move quickly to get better tools in their networks that can analyze traffic patterns on the fly and identify any unusual activity, said another expert in retail security, who has audited POS systems to find vulnerabilities that hackers can exploit. The expert said it is more difficult for small-to-mid sized retailers to do this because they do not have as much money and expertise as major retailers. The FBI report said the bulk of the POS malware cases that the agency has investigated involve small-to-mid sized local or regional businesses, whose estimated losses each range from tens of thousands of dollars to millions of dollars. The United States Secret Service usually takes the lead in credit card breach investigations for the federal government, though the FBI sometimes opens its own cases or asked to assist. The Secret Service is leading the investigations into the breaches at Target and Neiman Marcus. To read more click **HERE**

CNN's website and Twitter account hacked by Syrian Electronic Army

Yahoo, 24 Jan 2014: The Twitter account and website for CNN appeared to have been hacked on Thursday by individuals representing the Syrian Electronic Army (SEA). A number of suspicious tweets were posted to CNN's 11.6 million followers that included allegations that the CIA is behind the al-Qaida network. "Syrian Electronic Army Was Here … Stop lying … All your reports are fake!" reads one missive posted to the site. All of the tweets purporting to have been from the pro-Assad group were deleted within 10 minutes. The company's website also appeared to have been hacked and contained a false message. "Some of the organization's social media accounts were compromised via a third-party social publishing platform," CNN spokesman Matt Dornic told Yahoo News via email. "We are working with the affected users and vendor to remedy the issue." The SEA has successfully orchestrated more than two dozen high-profile hacking efforts going back to July 2011, including on the BBC, National Public Radio, Al-Jazeera and the Washington Post. Two of the other messages posted to the CNN Twitter account by Syrian hackers (Twitter). Though reportedly not directly affiliated with the Syrian regime, the SEA describes itself as being composed of "patriotic" young Syrians who are protesting how the Assad government has been portrayed since the onset of their country's civil war. The group achieved its greatest notoriety in April 2013, when it hacked the Associated Press Twitter account, announcing that the White House had been attacked and that President Obama had been injured. Though the false claim was almost immediately refuted, it still had a steep impact on the daily financial markets, causing a $136.5 billion temporary drop. The CNN hack was the second high-profile attack from SEA this week alone. On Monday, SEA reportedly hacked the official Microsoft blog. To read more click **HERE**

Hacker Claims to Have Breached Documentation Section of WHMCS Website

SoftPedia, 24 Jan 2014: A hacker who uses the online moniker "b0x," an administrator of the MadLeets forum, claims to have breached the website of client management, billing and support solutions provider WHMCS. E Hacking News informs that the hacker has uploaded an HTML file to the documentation section of the WHMCS site (docs.whmcs.com/images/b0x.html). At the time of writing, the page uploaded by the hacker is still online. A mirror of the file is available on zone-h.org. It's worth noting that the file appears to have been on the WHMCS site since January

12. I've sent an email to WHMCS to see if they can provide any clarifications, but so far, I haven't received a response. In May 2012, WHMCS was targeted by members of the notorious UGNazi group. At the time, the hackers claimed to have attacked the organization because it provided services to scammers and cybercriminals. Update. WHMCS representatives have provided the following statement: "Our system admin team just evaluated the server and b0x.html had a timestamp dating back to 2012. At the current time it is our belief that this was the result of a previous vulnerability related to mediawiki and no defacement has taken place. The MediaWiki software houses our documentation for WHMCS and does not have any hooks or sensitive data beyond public documentation for the WHMCS product." To read more click **HERE**

Easton-Bell Sports Vendor Suffers Data Breach, 6,000 People Reportedly Impacted
SoftPedia, 24 Jan 2014: Sports equipment and clothing maker Easton-Bell Sports has admitted suffering a data breach. The company says that cybercriminals have planted a piece of malware on the servers of a vendor. In a letter sent out to customers starting last week, Easton-Bell Sports reveals that the attackers might have obtained names, addresses, phone numbers, email addresses, credit card numbers and their associated security codes. The breach took place around December 1, 2013 and it was discovered only on January 9, 2014. It's believed that those who made purchases online between December 1 and December 31, 2013 are impacted. The precise number of victims has not been disclosed by the company, but Reuters reports that around 6,000 people made purchases online in December. Affected customers are being offered one free year of identity protection services. To read more click **HERE**

Microsoft: Disconnecting Windows XP from the Internet Won't Keep You Secure
SoftPedia, 23 Jan 2014: There are many ways to keep a Windows XP system secure after Microsoft officially stops releasing updates and security patches in April, but cutting off the Internet connection isn't one of them. That's what Redmond is saying in an internal document delivered to partners that are supporting the transition to another operating system, emphasizing that even without Internet access, a Windows XP machine could still be vulnerable to other types of attacks. "Being disconnected to an internal network [sic], or using a USB or CD to transfer information, may reduce the attack surface but will still leave you vulnerable to several types of attacks once support ends. Aside from a few special situations, keeping your Windows XP machine in a sealed room on its own is not the right choice for your business," Microsoft said in the documents obtained by CRN. Microsoft then goes on to say the same thing it explained with every single occasion: staying on Windows XP after retirement exposes all your data because hackers and cyber criminals would clearly attempt to exploit vulnerabilities found in the operating system and unpatched by the parent company. "We won't sugarcoat it: If you are running Windows XP after April 8, 2014, you are putting your business at risk -- and please don't believe anyone who claims that quick fixes can replace a critical OS update," the company added. Microsoft wants most Windows XP users to move from the old operating system to Windows 8.1, which is said to be the most secure and the fastest Windows version to date. Unfortunately, moving from Windows XP to 8.1 also involves hardware upgrades, which in many cases aren't possible due to the high costs of the entire process. Businesses and companies are clearly the ones most affected by Windows XP's demise, so with only three months on the clock, a decision needs to be made as soon as possible. To read more click **HERE**

Neiman Marcus says security breach may affect up to 1.1 million cards
Associated Press, 24 Jan 2014: Neiman Marcus says 1.1 million debit and credit cards used at its stores may have been compromised in a security breach last year. The high-end retailer said Visa, MasterCard and Discover have found 2,400 Neiman Marcus and Last Call customer cards that were used fraudulently. Last Call is Neiman Marcus' clearance chain. Neiman Marcus says it is notifying all customers who shopped in its stores in 2013 and offering them a free year of credit monitoring and identity-theft protection. Malicious software installed in Neiman Marcus' system attempted to take customer card information from July 16 to Oct. 30, the company said. The malicious software has been disabled. Neiman Marcus Group Ltd. reiterated in a post on its website Wednesday night that social security numbers and birth

dates were not stolen and customers who shopped online were not affected. Customers that use its private Neiman Marcus credit cards were also not affected. The Dallas-based company said the investigation is ongoing. The company learned that malicious software was installed to its system on Jan. 1, after a forensics company discovered it. It informed federal law enforcement agencies and began working with the U.S. Secret Service and payment processors. Neiman Marcus said it has no knowledge of a connection between the two security breaches. A report published earlier this month by iSight Partners, a global cyber intelligence firm that works with the U.S. Secret Service and the Department of Homeland Security, said the security breach that hit Target appears to have been part of a broader and highly sophisticated scam that potentially affected a large number of retailers. To read more click **HERE**