The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

30 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

January 28, Wired.com – (International) **Coder behind notorious bank-hacking tool pleads guilty.** A Russian man extradited from the Dominican Republic pleaded guilty in an Atlanta court to developing, selling, and customizing the SpyEye banking trojan that infected more than 1.4 million computers. The trojan was sold to over 150 customers worldwide who used it to compromise thousands of bank accounts and steal millions of dollars. Source: http://www.wired.com/threatlevel/2014/01/spy-eye-author-guilty-plea/

January 27, KSLA 12 Shreveport – (Louisiana) **$20,000 worth of iPads stolen from Caddo elementary school.** Police are investigating after about $20,000 worth of iPads were stolen from Oak Park Elementary School in Shreveport. Source: http://www.ksla.com/story/24558951/20000-worth-of-ipads-stolen-from-caddo-elementary-school?hpt=ju_bn2

January 29, Help Net Security – (International) **VPN bypass attack possible also on Android KitKat.** Security researchers at Ben Gurion University found that a previously-reported VPN bypass vulnerability in Android 4.3 was also able to be modified and used on devices running Android 4.4 'KitKat.' Source: http://www.net-security.org/secworld.php?id=16277

January 29, Softpedia – (International) **Rovio confirms hackers defaced Angry Birds website, no user data compromised.** Rovio confirmed that hacktivists briefly defaced the Web site of the Angry Birds game via DNS hijacking but did not compromise any user data. Source: http://news.softpedia.com/news/Rovio-Confirms-Hackers-Defaced-Angry-Birds-Website-No-User-Data-Compromised-421857.shtml

January 28, Softpedia – (International) **Java bot can launch DDoS attacks from Windows, Mac and Linux machines.** Researchers at Kaspersky identified a malicious Java application designed to perform distributed denial of service (DDoS) attacks that can run on Windows, Linux, and Mac OS computers dubbed HEUR:Backdoor.Java.Agent.a. The malware is believed to have been used to attack a bulk email service. Source: http://news.softpedia.com/news/Java-Bot-Can-Launch-DDOS-Attacks-from-Windows-Mac-and-Linux-Machines-421551.shtml

January 28, Softpedia – (International) **Patnote virus used to distribute ZeuS trojan.** Trend Micro researchers discovered a malware distribution campaign using the Patnote virus to spread the ZeuS malware. The virus adds its code to all executable files in a system and on removable and network drives, and contains mechanisms to prevent it from being analyzed. Source: http://news.softpedia.com/news/Patnote-Virus-Used-to-Distribute-ZeuS-Trojan-421468.shtml

Nigerian Scammers Are Increasingly Targeting LinkedIn Users
SoftPedia, 30 Jan 2014: Security experts from Bitdefender warn that Nigerian scammers are increasingly targeting users of the professional social media network LinkedIn. The cybercrooks are creating fake accounts and sending out typical 419 messages to users. In an example spotted by Bitdefender, the scammers pretend to be the CEO of a petrochemical company from

Kuwait called Equate. The scam messages contain correct contact information from the company, except for the PO box and the CEO's email address, which of course, is on a private email service. The scam messages read something like this: "I am Mohammad Hussain the president & CEO Equate Petrochemical company Kuwait. I write to request your co-operation in my desire to find a foreign partner who will assist me in the relocation and Transfer of some amount of money which I have made available for investment purpose abroad to offer to secure the future of my children after retirement." Equate is aware of this scam. The company has posted an alert on its website to warn customers of the scammy emails. "Equate does not send out emails soliciting business and assumes no responsibility/liability. Therefore, please ignore such emails and report to ccd@equate.com," the alert reads. Bitdefender says scammers also pretend to be employees of NatWest and Standard Chartered Bank. Mostly, Nigerian scams are the same as they've always been. The scammers try to trick victims into sending them money after promising them the chance to make millions. The money sent by the victims is allegedly needed to complete the transaction. However, as all cybercriminals, those who launch 419 scams keep up with the times and use various tricks to increase their chances of success. In this case, they've started to abuse LinkedIn. Since many LinkedIn users are looking for business opportunities, some might fall for these scams. To read more click HERENigerian Scammers Are Increasingly Targeting LinkedIn Users SoftPedia, 30 Jan 2014: Security experts from Bitdefender warn that Nigerian scammers are increasingly targeting users of the professional social media network LinkedIn. The cybercrooks are creating fake accounts and sending out typical 419 messages to users. In an example spotted by Bitdefender, the scammers pretend to be the CEO of a petrochemical company from Kuwait called Equate. The scam messages contain correct contact information from the company, except for the PO box and the CEO's email address, which of course, is on a private email service. The scam messages read something like this: "I am Mohammad Hussain the president & CEO Equate Petrochemical company Kuwait. I write to request your co-operation in my desire to find a foreign partner who will assist me in the relocation and Transfer of some amount of money which I have made available for investment purpose abroad to offer to secure the future of my children after retirement." Equate is aware of this scam. The company has posted an alert on its website to warn customers of the scammy emails. "Equate does not send out emails soliciting business and assumes no responsibility/liability. Therefore, please ignore such emails and report to ccd@equate.com," the alert reads. Bitdefender says scammers also pretend to be employees of NatWest and Standard Chartered Bank. Mostly, Nigerian scams are the same as they've always been. The scammers try to trick victims into sending them money after promising them the chance to make millions. The money sent by the victims is allegedly needed to complete the transaction. However, as all cybercriminals, those who launch 419 scams keep up with the times and use various tricks to increase their chances of success. In this case, they've started to abuse LinkedIn. Since many LinkedIn users are looking for business opportunities, some might fall for these scams. To read more click **HERE**

Fake Google "Suspicious Sign-In Prevented" Emails Lead to Phishing Site

SoftPedia, 30 Jan 2014: Google customers are advised to be on the lookout for fake notifications that inform them of suspicious login attempts. Experts have found that such emails are being sent out by cybercriminals to lure users to phishing sites. The emails are entitled "Suspicious sign-in prevented" and they read something like this: "Someone recently used wrong passwords to try to sign in to your Google Account. We prevented the sign-in attempt in case this was a hijacker trying to access your account. Please review the details of the sign-in attempt. If you do not recognize this sign-in attempt, someone else might be trying to access your account. You should check activity immediately." The main problem with this phishing attack is that Google actually sends users such emails in case suspicious login attempts are detected. However, cybercriminals have also been sending out such emails over the past years. In some cases, the bogus notifications are utilized to distribute malware, while in others, to lure people to phishing sites. In this particular case, brought to our attention by a security researcher of Malwared.ru, internauts are taken to a phishing site hosted on privacy.google-settings.com. The domain might look legitimate at first sight, but it's not owned by Google. The expert says that it has been registered by one Aksnes Thomas from Sweden, with the email address aksnes.thomas@yahoo.com. The phishing site's source contains an email address, valsowrom@gmail.com, which the

researcher believes could be the attacker's address. If you come across such emails, analyze them carefully before clicking on any of the links or buttons. Make sure that the links point to a legitimate Google domain, such as gmail.com, mail.google.com or accounts.google.com before entering your credentials. If you're a victim of this phishing attack, change your password as soon as possible. If you've been using the same password for multiple accounts, change it for those as well. To read more click **HERE**

Target Says Hackers Breached Its Systems after Stealing Credentials from a Vendor

SoftPedia, 30 Jan 2014: The cybercriminals that stole the details of 40 million payment cards and the contact information of 70 million Target customers are said to have breached the retailer's systems after stealing credentials from a vendor. What we have known so far is that the attackers gained access to information on point-of-sale registers by planting a piece of malware. However, it hasn't been known how the malware got there in the first place. Target representatives have told The Wall Street Journal that the attackers had stolen credentials from a vendor and used the information to access the company's systems. The vendor has not been named and it's uncertain how the hackers obtained the data. It's also uncertain which of Target's portals allowed them to gain access to payment systems. WSJ has also reported that the retailer shut down a couple of its portals: a supplier's database and a human resources website. To read more click **HERE**

@N Hack: GoDaddy Admits Employee Had Been Social Engineered, PayPal Denies It

SoftPedia, 30 Jan 2014: On Wednesday, we learned that a hacker managed to hijack the coveted @N Twitter username after extorting its owner into handing it over. The former owner of the account, Naoki Hiroshima, has blamed PayPal and GoDaddy for the incident. He claims the hacker gained access to his GoDaddy account after social engineering an employee with the aid of information handed over to him by PayPal staff. More precisely, the attacker requested and obtained partial credit card data. Both GoDaddy and PayPal have issued statements regarding the incident. GoDaddy admits that one of its employees had been tricked into providing the hacker the information needed to access Hiroshima's account. However, the hosting giant says the cybercriminal already possessed a large portion of the customer information needed to access the account when he contacted the company. "The customer has since regained full access to his GoDaddy account, and we are working with industry partners to help restore services from other providers," stated GoDaddy Chief Information Security Officer Todd Redfoot. "We are making necessary changes to employee training to ensure we continue to provide industry-leading security to our customers and stay ahead of evolving hacker techniques." While GoDaddy has accepted partial responsibility for the account takeover, PayPal hasn't. The payment processor says that it has launched an investigation after Hiroshima published his post. PayPal admits that there have been failed attempts to obtain a customer's information. However, according to their statement, "PayPal did not divulge any credit card details related to this account. PayPal did not divulge any personal or financial information related to this account. This individual's PayPal account was not compromised." The company says that its employees are well trained when it comes to handling social engineering attempts. PayPal says that it's trying to reach out to Hiroshima to assist him. To read more click **HERE**

Lenovo Acquires Google's Motorola Mobility for $2.91 Billion

REMINDER: Lenovo is a Chinese-owned company

SoftPedia, 30 Jan 2014: It looks like what started as a rumor earlier today proved to be 100% accurate, as Lenovo and Google have just announced they have reached an agreement for the acquisition of Motorola Mobility smartphone business. Google purchased Motorola Mobility back in 2011 for $12.5 billion (€9.15 billion) and the agreement it has reached today with Chinese company Lenovo mentions it will only get $2.91 billion (€2.13 billion) for the company. That means Google has decided to sell Motorola at a huge loss. Even though the Motorola Mobility's smartphone business shrank over the years due to layoffs and closing of operations in almost all countries except the United States and Canada, the selling price is still far from what Google originally paid for it. The good news for Google is that the search

giant will keep most of Motorola's patents, including current patent applications and invention disclosures, like Project Ara for example. Lenovo will still receive a license to Motorola's portfolio of patents and other intellectual property, along with over 2,000 patent assets, as well as the Motorola Mobility brand and trademark portfolio. Aside from the current smartphones Motorola is already successfully selling in various countries (Moto X and Moto G), Lenovo has also confirmed it will take ownership of the future Motorola Mobility's roadmap. Under agreement, Lenovo will pay $1.41 billion (€1.03 billion) at close, comprised of $660 million (€483 million) in cash and $750 million (€549 million) in Lenovo ordinary shares (subject to a sharecap/floor). Furthermore, the remaining $1.5 billion (€1.1 billion) will be paid in the form of a three-year promissory note. "The acquisition of such an iconic brand, innovative product portfolio and incredibly talented global team will immediately make Lenovo a strong global competitor in smartphones. We will immediately have the opportunity to become a strong global player in the fast-growing mobile space," said Yang Yuanqing, chairman and CEO of Lenovo. "Lenovo has the expertise and track record to scale Motorola Mobility into a major player within the Android ecosystem. This move will enable Google to devote our energy to driving innovation across the Android ecosystem, for the benefit of smartphone users everywhere," said Larry Page, CEO, Google. "As part of Lenovo, Motorola Mobility will have a rapid path to achieving our goal of reaching the next 100 million people with the mobile Internet. With the recent launches of Moto X and Moto G, we have tremendous momentum right now and Lenovo's hardware expertise and global reach will only help to accelerate this," said Dennis Woodside, CEO, Motorola Mobility. To read more click **HERE**

Two Pieces of Malware Used in Neiman Marcus Cyberattack

SoftPedia, 29 Jan 2014: Earlier this month, high-end retailer Neiman Marcus admitted suffering a data breach in which payment card data was compromised. The company says that around 1.1 million card numbers are impacted. In a letter sent earlier this week to the New Hampshire Attorney General's Office, Tracy Preston, senior vice president and general counsel of the Neiman Marcus Group, revealed that two pieces of malware had been used in the attack. The piece of malware responsible for stealing Track 1 information from cards, the "scraping malware," was planted on the retailer's systems in July 2013. The threat was active between July and October 2013, but not every day during this period and not at all stores. In this timeframe, a total of 1.1 million credit cards were used at the firm's stores. However, Neiman Marcus has also learned that this piece of malware couldn't have functioned without another malicious element that had made its way onto the company's networks earlier in 2013. "Separate, related malware that allows this scraping malware to function appears to have been clandestinely inserted earlier in 2013. Neiman Marcus was not aware of any of this hidden malware until it was discovered this month by our investigative experts," Preston noted in her letter. Around 2,400 payment cards used at Neiman Marcus stores have been used for fraudulent transactions. However, it's uncertain if all the information was obtained from the high-end retailer, since the cards could have been used at other companies that were targeted by cybercriminals. Neiman Marcus has contact information for 71% of these individuals. The firm says that it has made public statements in order to inform those for whom it doesn't have contact details. Free credit monitoring services are being offered to all those who shopped at Neiman Marcus between January 2013 and January 22, 2014. To read more click **HERE**