The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

3 February 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 31, Softpedia – (International) **Tor-based malware ChewBacca used to steal card data from POS systems.** Researchers at RSA found that the ChewBacca trojan has been used to log track 1 and track 2 data from compromised point-of-sale (POS) systems since October 2013 in attacks targeting dozens of retailers. Source: http://news.softpedia.com/news/Tor-Based-Malware-ChewBacca-Used-to-Steal-Card-Data-from-POS-Systems-422634.shtml

January 31, Softpedia – (International) **Experts find 28 security issues in Oracle's Java Cloud Service.** Researchers at Security Explorations analyzed Oracle's Java Cloud Service and found 28 security issues, 16 of which could be leveraged to bypass the Java security sandbox of a targeted WebLogic server environment. The vulnerabilities could also be leveraged to gain access to deployments of other users in the same regional data center, according to the researchers. Source: http://news.softpedia.com/news/Experts-Find-28-Security-Issues-in-Oracle-s-Java-Cloud-Service-422629.shtml

January 31, Help Net Security – (International) **Yahoo Mail accounts compromised in coordinated attack.** Yahoo reported January 30 that attackers attempted to access a large number of Yahoo Mail accounts using usernames and passwords likely obtained from a third-party database breach. Yahoo reset passwords for affected accounts and advised users to secure their accounts by changing their passwords. Source: http://www.net-security.org/secworld.php?id=16289

January 30, Softpedia – (International) **Service promising Twitter followers hijacks accounts and uses them for spam.** A service promising to increase a user's Twitter followers was found by Trend Micro researchers to hijack users' accounts to send out spam. Source: http://news.softpedia.com/news/Service-Promising-Twitter-Followers-Hijacks-Accounts-and-Uses-Them-for-Spam-422236.shtml

January 30, SC Magazine – (International) **GoDaddy admits giving up info that led to Twitter username extortion.** GoDaddy reported that an attacker with personal information of the owner of a rare Twitter account name was able to use social engineering to access the account holder's GoDaddy account over the phone as part of an extortion scheme to steal the Twitter account. Source: http://www.scmagazine.com/godaddy-admits-giving-up-info-that-led-to-twitter-username-extortion/article/331867/

eBay and PayPal UK domains hacked by Syrian Electronic Army
ZDnet, February 2, 2014: Hacking group Syrian Electronic Army today breached and defaced websites belonging to PayPal UK and eBay, though each website was resolving without issue or defacement after the announcement was made. The SEA provided its evidence on Twitter, with an example of what appeared to be PayPal.co.uk's website with a fresh deface, and a second follow-up tweet labeled "Internal Paypal communications confirming penetration." The Twitter account used by the Syrian Electronic Army for the announcement has since been suspended. PayPal confirmed the security breach telling ZDNet via email, "PayPal's Sr. Director of Global Initiatives notes that the problem was limited to marketing pages in the UK, France, and India

redirecting, that it has been resolved, and no user data was compromised." PayPal did not provide an explanation regarding the display of its paypal.co.uk URL in the evidence of the hack as provided by the Syrian Electronic Army. Nor did PayPal address the eBay UK forum members who tried to visit eBay.co.uk and experienced what they described as an hour-long outage of eBay's primary UK website from a Syrian Electronic Army attack. The defacement purported to be on PayPal.co.uk read, "Hacked by the Syrian Electronic Army. Long live Syria. F*ck the United States government." The Syrian Electronic Army Twitter account directly addressed the concerns of PayPal users that the attack was political and not intended for theft saying, "Rest assured, this was purely a hacktivist operation, no user accounts or data were touched." It tweeted saying, "For denying Syrian citizens the ability to purchase online products, Paypal was hacked by the #SEA." The focus was on PayPal's UK site. PayPal UK offers a donation page for Syrian relief efforts, but the country is not on its page of supported countries. PayPal does not support use of its services in Syria -- this also affects eBay buyers -- and it is widely considered that Syria is held on a blacklist of omission that includes dozens of other countries including Afghanistan, Haiti, American Samoa, Cuba, Pakistan, Libya, Sudan and many more. It is unclear how the attack occurred. The SEA told Hackread, Paypal used a large amount of authentication and verification protocols so the attack required a lot more advanced techniques. For those living in any of PayPal's blacklisted countries, making simple online transactions is very hard and PayPal's blacklist makes it nearly impossible to enter into the most basic forms of online business. To read more click **HERE**

Kaspersky to Reveal Details of Sophisticated Cyber Espionage Operation "The Mask"
SoftPedia, 2 Feb 2014: Next week, at the Kaspersky Security Analyst Summit 2014, researchers will present their findings on another highly sophisticated cyber espionage campaign that Kaspersky has dubbed "The Mask." According to experts, the cybercriminals behind The Mask have been in operation since 2007. They've targeted victims in a total of 27 countries. The advanced persistent threat (APT) actors are relying on extremely sophisticated malware that's said to be even more advanced than the notorious Duqu. The tools used by the attackers include a bootkit, a rookit, Mac OS and Linux versions of the malware, and even components specially designed for attacks against Kaspersky products. Another noteworthy detail about The Mask campaign is that the cybercriminals speak a language that has been "observed very rarely in APT attacks." To read more click **HERE**

Details of 800,000 Orange Customers Compromised in Hack Attack
SoftPedia, 2 Feb 2014: On January 16, cybercriminals hacked into the systems of telecoms giant Orange. The attackers targeted the My Account section of the orange.fr website. According to PC INpact, the hackers have gained access to names, mailing addresses, email addresses, phone numbers and other information. Orange representatives say that less than 3% of their customer base is impacted by the attack, more precisely around 800,000 individuals. Shortly after detecting the attack, Orange shut down the My Accounts page. Impacted individuals are being notified via email. Orange Technical Director Laurent Benatar has clarified that passwords have not been compromised, not even encrypted ones. The cybercriminals might have gained access to some partial financial information. Benatar explains that sensitive data such as bank account numbers are redacted, the full versions being stored on separate servers that haven't been impacted by this breach. The announcement comes after Orange warned customers of phishing emails on January 23, 24. At the time, the telecoms company didn't mention anything about a cyberattack. The phishing warnings should be taken seriously since the cybercriminals can leverage the stolen information for targeted attacks. To read more click **HERE**

Hackers Claim to Have Breached Bell Canada's Systems
SoftPedia, 1 Feb 2014: Hackers of the NullCrew collective are back. They claimed to have breached the systems of Bell Canada. The details of thousands of users have been leaked online. "Go [expletive] figure, people who are supposed to provide secure connection to the internet? They can't secure themselves," the hackers wrote next to the data leaked on the group's website. There are tens of thousands of pieces of information, including usernames, email addresses,

passwords, and even some credit card data. Cyber War News has analyzed the data and found that there are credentials which appear to be associated with various Bell services. I've sent an email to Bell Media to see if they can provide any clarifications regarding the incident. I'll update this post if they respond to my inquiry. Update. Bell Canada has confirmed that the leaked data belongs to its customers, but the company says its own systems have not been hacked. To read more click **HERE**

Hotel Management Company White Lodging Suffers Data Breach

SoftPedia, 1 Feb 2014: White Lodging, a hotel management company whose portfolio includes Westin, Marriott, Hilton and Sheraton, has suffered a data breach in which thousands of payment cards might have been compromised. According to Brian Krebs, the banking industry has detected hundreds of fraudulent transactions on cards used at various Marriott hotels since March 23, 2013. The affected hotels are in Tampa, Chicago, Austin, Los Angeles, Denver and Louisville. The one thing these hotels have in common is that they're managed by White Lodging. It's worth noting that the compromised payment cards have been used at restaurants and gift shops from within the impacted hotels, not at front desks, which use Marriott's own property management systems. White Lodging has told Krebs that they're investigating the reports. Meanwhile, Marriott has also launched an investigation, but the company highlights the fact that its own systems have not been compromised. News of this incident comes shortly after a number of US retailers admitted suffering data breaches in which credit and debit cards had been stolen by cybercriminals. The list includes Target, Neiman Marcus and Michaels Stores. To read more click **HERE**

Russian Man Sentenced to 30 Months in Jail for Hacking Trading Accounts

SoftPedia, 1 Feb 2014: Petr Murmylyuk, 33, a Russian national living in Brooklyn, New York, has been sentenced to 30 months in prison for taking part in a securities fraud scheme that involved hacking into trading accounts. He has also been sentenced to three years of supervised release and ordered to pay $505,357.79 (€374,866.83) in restitution. The sentence comes after Murmylyuk pleaded guilty to conspiracy to commit securities fraud. According to the FBI, Murmylyuk and others hacked into the online accounts of the customers of various brokerage companies, including E*Trade, Schwab, Scottrade and Fidelity. The information obtained from the hijacked accounts was used to open new accounts at other brokerage firms. They made a profit by making unprofitable and illogical security trades between the victim's account and the newly created ones, which they dubbed "profit accounts." "One version of the fraud involved causing the victims' accounts to sell options contracts to the profit accounts and then to purchase the same contracts back minutes later for many times the price," the FBI revealed. In order to avoid triggering the security mechanisms designed to inform the victims in case of suspicious transactions, the fraudsters changed the email addresses and phone numbers associated with the targeted accounts. The illegal proceeds were deposited into the bank accounts of foreign nationals who came to the US for various reasons. These individuals were recruited by the fraudsters especially for this purpose. The targeted brokerage firms are said to have suffered losses of around $1 million (€730,000). Murmylyuk was arrested in November 2011 and was charged in April 2012. The list of US government organizations involved in this investigation includes the FBI, the ICE, the HIS, and the IRS. The Financial Fraud Enforcement Task Force that US President Barack Obama established in an effort to combat financial crimes has been credited for this prosecution. To read more click **HERE**

How COTS endangers national security

Federal Times, 29 Jan 2014: I have long said that if you look at all the disclosures of cyber attacks and breaches, you may not have an accurate view of the current state of this national security threat. Well, last year CNBC posted a piece titled "Cyberattacks: Why Companies Keep Quiet [**LINK**]" that expressed the same concern. I was involved in a discussion recently about the disclosure requirements that apply when publically traded companies experience a cyber breach. The rule of thumb for the breach or cyber attack to require disclosure - it would have to be "material" (an accounting term). The Journal of Accounting states that "materiality" is based on an assumption that a fluctuation in net income of 5

percent or less is unlikely to influence a reasonable investor. Take a look at the revenue of those in the defense industry and just how significant the costs of the attack would have to be before it needs to be disclosed. That would explain the limited number of disclosures we see. Do you think this might be what is behind the Securities and Exchange Commission's (SEC) decision to "Focus on Corporate Cybersecurity Risks in 2014? [**LINK**]" If you examine how much of our military equipment falls into the COTS (commercial off the shelf) category as well as how much of our critical infrastructure is operated by the private sector in addition to all the commercial equipment they use, you can see the danger of companies and the supply-chain being compromised by counterfeit equipment or products with built in malicious code. This is a critical issue! Supply-chain security has increasingly become an area of deep concern for the DoD, the government and the private sector. The Brookings Institution published a report [**LINK**] that focuses on compromised electronic components. In their executive summary they state "supply chain is almost completely unprotected." To read more click **HERE**

Million-dollar bank hacking kit Russian developer pleads guilty to charges in US

ANI, Washington, Jan. 30, 2014: The Russian man who developed malware kit for some of the web's most expensive banking hacks has reportedly pleaded guilty to the charges. 24-year-old Aleksander Panin pleaded guilty for developing the SpyEye malware kit, which was considered one of the biggest malware threats and was used for major banking hacks. According to The Verge, Panin made his money by selling the exploit kit to more daring criminals, more than 150 different clients who used the readymade software to take on banking sites. One of his clients used the malware to infect as many as 1.4 million computers in a banking attack and walked away with over 3 million dollars. The report said that Panin's downfall came when he sold a copy of the malware kit to a federal agent in mid-2011 and his arrest came more than two years later. Panin faces up to 30 years in prison. To read more click **HERE**

Trustwave Demonstrates Malware That Logs Touchscreen Swipes to Record Your PIN

Forbes, 27 Jan 2014: Neal Hindocha, a senior security consultant for Trustwave, has built proof-of-concept 'screenlogging' malware that monitors finger swipes on smart devices in combination with taking screenshots, painting a picture of exactly how the user is interacting with their phone or tablet. Hindocha's concept malware logs the X and Y coordinates of any swipe or touch. Speaking with Forbes, Hincocha says it wasn't much hassle to get the code running on jailbroken iOS and rooted Android devices, and that it's possible to get it working on regular Android smartphones, provided they are plugged into a PC – for example, while charging by USB. Trustwave was examining financial malware on the Windows platform and wanted to see if similar methods could be applied to mobile. Keylogging has been a typical component for financial Windows malware, and there are apps that already log keyboard inputs on smart devices. But Hindocha says the finance industry is moving away from using typical keyboard inputs, whether it is with a PIN code or another kind of password. Recording touch screen coordinates "has a certain value in itself," Hindocha says. "If you're monitoring all touch events and the phone hasn't been touched for at least one hour, then you get a minimum of four touch events, you can assume that is a PIN code being entered." "The more interesting thing is, if you get a screenshot and then overlay the touch events, you're looking at a screenshot of what the user is seeing, combined with dots, sequentially, where the user is touching the screen." The end result, Hindocha explains, is that it doesn't matter how a user inputs the information: all of it is going to be captured. It's also possible to figure out where on the device the user is at a given time – you can set the code to take screenshots only when a user is in an app rather than on the home screen to avoid racking up a lot of disk space. Hindocha hopes that by demonstrating his concept at the upcoming RSA Security conference, he will help make app developers and companies with high security requirements understand the importance of issues that, if ignored, could potentially leave people or businesses wide open. To read more click **HERE**

FBI warns retailers about the increasing threat of cyberattacks

Security InfoWatch, 27 Jan 2014: The FBI is warning retailers to be on alert for more cyber-attacks involving malicious software used to steal customers' credit and debit card data as luxury retailer Neiman Marcus yesterday disclosed that more than 1 million customers' cards may have been compromised. A Jan. 17 FBI report describes risks posed by "memory-parsing" malware that's infected companies' point-of-sale systems in about 20 hacking cases in the past year, Reuters reported yesterday. "We believe POS malware crime will continue to grow over the near term, despite law enforcement and security firms' actions to mitigate it," the FBI report said, according to 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." Neiman Marcus disclosed Jan. 10 that hackers may have stolen its customers' credit and debit card information. As of yesterday, Visa, MasterCard and Discover had notified the Dallas company that about 2,400 cards used at Neiman Marcus and Last Call stores were subsequently used fraudulently, Neiman Marcus Group CEO Karen Katz disclosed in a letter on the company's website. "It appears that the malware actively attempted to collect or 'scrape' payment card data from July 16, 2013, to October 30, 2013," she said. Target Corp. said last month that the credit and debit card data of up to 40 million customers had been accessed by hackers in a malware attack, and this month said personal information of 70 million customers also was accessed. Consumers can expect more merchants admitting breaches in the near future, because their Internet protocol addresses, logins and passwords are being sold on the black market, said Dan Clements, president of IntelCrawler, a cyber-intelligence firm. "It has a level of sophistication where the Target (breach) would not have shocked you," he said. Criminals are advertising them for as little as $25, and throwing in malware already loaded on merchants' systems for $100, according to Clements. "It's very, very low-risk and a high return," he said. "It's just simple economics." To read more click **HERE**

Hackers break into Israeli defence computers, says security company

Heise Security, 27 Jan 2014: Hackers broke into Israeli defence ministry computers via an email attachment tainted with malicious software, according to an Israeli cyber-security company. Aviv Raff, chief technology officer at Seculert, said the hackers temporarily took over 15 computers this month, one of them belonging to Israel's civil administration, which monitors Palestinians in Israeli-occupied territory. The email attachment looked as if it had been sent by the country's Shin Bet secret security service. Raff said Palestinians were suspected of being behind the cyber-attack, citing similarities to an attack on Israeli computers more than a year ago from a server in the Hamas-ruled Gaza Strip. While the latest attack was conducted from a server in the US, experts noticed writing and composition similarities with the earlier attack, he said. Israeli officials declined to comment on Raff's findings. "We are not commenting on it. We don't respond to such reports," said Guy Inbar, a spokesman for the civil administration. Seculert had not determined what the hackers did after the initial infection with Xtreme RAT software, Raff said. "All we know is at least one computer at the civil administration was in control of the attackers; what they did we don't know." The civil administration is a unit of Israel's defence ministry, which oversees the passage of goods between Israel and the West Bank and Gaza Strip, territories Israel captured in the 1967 war and which Palestinians want for a state. The administration also issues entry permits to Palestinians who work in Israel. Raff declined to identify the other 14 computers targeted by the hackers. An Israeli source said these included companies involved in supplying Israeli defence infrastructure. Based on Raff's analysis, the 15 computers were in the hackers' grip for at least several days after the dispatch on 15 January of the email, which included an attachment about Ariel Sharon, the former prime minister, who had just died. Hacking activity has surged in the Middle East in the past three years as governments and activist groups target the military, other state agencies, critical infrastructure, businesses as well as dissidents and criminal groups in order to gain information about their operations and disrupt them. Raff's company was able to "sinkhole" the operation this month, tricking the Xtreme RAT software into communicating with servers that Seculert controlled in order to discover which computers were infected and to deactivate the attack. Xtreme RAT is a remote access trojan that gives hackers complete control of an infected machine. They can steal information, load additional malicious software on to the network or use the

compromised computer as a beachhead from which to conduct reconnaissance and attempt to gain deeper access into the network, Raff said. News of the cyber-attack came a day before a three-day Israeli cybertech conference being held in Jerusalem, and just after Prime Minister Binyamin Netanyahu plugged Israeli technological advances at the World Economic Forum in Davos. Raff denied that there was any irony in the timing of his warning so soon after Netanyahu's remarks. "Unfortunately there is no such thing as 100% safety either when it comes to physical risks or information security," he said. To read more click **HERE**

Punish careless employees to reduce security breaches, vendor says

Computerworld, 27 Jan 2014: Security could be vastly improved by holding employees accountable for carelessly clicking on emailed links and attachments that lead to malware being downloaded to a corporate network, an awareness-training vendor says. Rather than simply re-training employees who are prone to fall for phishing attacks, KnowBe4 advocates reporting those to immediate supervisors and human resource departments that can pressure workers into becoming more careful. "With this program, they start to understand that there truly are repercussions for clicking on phishing links," Stu Sjouwerman, founder and chief executive of KnowBe4, said. "That will change the behavior." KnowBe4's online program includes automatic notification of management when employees click on potentially malicious links in fake phishing attacks the company uses to periodically test employees after they have undergone training. Roughly 35 percent of the company's customers are financial institutions. To prove the effectiveness of accountability, KnowBe4 did a study on the employees of 372 companies over a 12-month period. Of the 291,000 people who underwent testing, the vendor found roughly 16 percent who were especially prone to click on links in bogus phishing email. KnowBe4 claims that once the test group was held accountable for how they handled email, the percentage still inclined to becoming victims of phishing attacks fell to just over 1 percent. "You have to be constantly reminding these people that they should not click on links, should not open attachments unless they know who it's from," Sjouwerman said. Phishing is the most popular method of hackers. The malicious email typically contains content that would make it appear legitimate to the recipient. For the second quarter of 2013, the latest numbers available, the Anti-Phishing Working Group reported a total of 639 company brands were used to disguise emails, with the names of payment services and financial institutions the most commonly used. To read more click **HERE**

Global cybercrime dominated by 50 core groups, CrowdStrike report finds

Computerworld, 24 Jan 2014: Cybercrime in 2013 was dominated by a core of around 50 active groups, including Russian and Chinese 'threat actors' whose activities are only now coming to light, a report from monitoring firm CrowdStrike has found. Using an approach that foregrounds the 'threat actors' above the malware itself, the firm divides groups according to whether they are deemed to be motivated primarily by national, political and purely commercial motives As CrowdStrike's marketing motto puts it: "you don't have a malware problem, you have an adversary problem." At first, the categorisation system looks more like a blizzard of inscrutable names, with major cyber-groups including 'Numbered Panda', 'Magic Kitten', 'Energetic Bear' and Deadeye Jackal. But the underlying system - it calls this methodology the 'cryptonym system' - is much simpler. Nation-state groups from China are always 'pandas', groups tied to politics rather than nation are 'jackals' and professional cybercriminals are always 'Spiders'. The most active groups included the Syrian Electronic Army (SEA) and a range of Chinese groups but this much was already known. More interesting, CrowdStrike thinks it has discovered a few that are less well documented, including 'Emissary Panda' and 'Energetic Bear', as their codenames would suggest the first being a Chinese group the second Russian. Emissary Panda appears to be a recently-formed group that goes after the high-tech sector, defence firms and embassies in a clutch of targets countries and a complement to the many other Chinese groups doing the same thing. More significant perhaps is Energetic Bear, which CrowdStrike believes has been going after energy-sector firms. Hitherto, Russia has been seen as the home of overwhelmingly commercial malware, indeed perhaps as the most active commercial cyber-criminal sector in the world bar none. Energetic Bear suggests that this could be changing as the Russian state takes a leaf out rival state-backed cyberjacking activities. Active since at least 2012 in 23 different

countries, Energetic Bear looks significant enough to have created 25 versions of one to its preferred Remote Access Trojans (RATs), Havex. Beyond energy firms, targets have included European governments and defence sector firms, engineering firms, and European, US and Asian academics, CrowdStrike said. The evidence for this group's Russian provenance included malware build times that corresponded to working hours in the country. Whether this means that this group is operating on behalf of the country's Government is impossible to say. "Whatever the motivation may be, having private groups carry out malicious activity has advantages for nation-states," said CrowdStrike, which listed a major motivation as being plausible deniability. "We have been tracking this threat actor for several years and the Energetic Bear objectives map to the Russian Federations use of natural resources as policy tool," said CrowdStrike's vice president of intellligence, Adam Meyers. To read more click **HERE**

Energy Sector under Attack

ISS Source, 23 Jan 2014: A cyber espionage campaign targeted hundreds of organizations from Europe, America and Asia and it appears the Russian government is behind it, researchers said. IT security firm CrowdStrike said Russia has been launching cyber attacks in an effort to steal sensitive information which it can use to gain an economic advantage over its opponents. CrowdStrike did not name the companies targeted by the Russian government, but the researchers said the list includes tech firms, energy providers, defense contractors, academia and even government agencies. CrowdStrike said the campaign primarily focuses on the energy sector. Researchers said a hacker group dubbed "Energetic Bear" has been operating on behalf of the Russian government. CrowdStrike monitored the team's operations since August 2012. CrowdStrike found the Russian government is behind the espionage campaign based on the technical indicators, the chosen targets and the data they went after and stole. The cybercriminal group has been relying on two Remote Access Trojans (RATs) in its operations: HAVEX RAT and SYSMain RAT. Technical details on the Energetic Bear attacks are in CrowdStrike's Global Threat Report for 2013. "Targeted entities and countries are consistent with likely strategic interests of a Russia-based adversary. Several infected hosts were observed within the Russian Federation, but this could be the result of accidental compromise through large-scale SWC operations or deliberate efforts to conduct domestic Internal monitoring," the report said. "Other data supporting a Russia-based adversary are observed in timing data related to these activities that aligns neatly with Russian working hours." Click **here** to register for the Crowdstrike report. To read more click **HERE**