THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

17 November 2014

Purpose
Educate recipients of cyber events to aid in protecting electronically stored DoD, corporate proprietary, and/or Personally Identifiable Information from theft, compromise, espionage

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, and Sandia National Labs

State Department's unclassified email system hacked

Reuters, 17 Nov 2014: The U.S. State Department's unclassified email systems were the victim of a cyberattack in recent weeks, around the same time as White House systems were breached, a senior U.S. official said on Monday. The official, who spoke on condition of anonymity, said none of the department's classified systems was compromised. Portions of its unclassified systems have been shut down to improve their security but should be back online shortly. "The department recently detected activity of concern in portions of its unclassified email system. "The department is implementing improvements to the security of its main unclassified network during a scheduled outage of some internet linked systems," the official added. "This has impacted some of our unclassified email traffic and our access to public websites from our main unclassified system. We expect our systems to be up and running soon." The U.S. official said the State Department breach was part of the same incident reported by the White House's Executive Office of the President (EOP) recently. The State Department's network was infiltrated last month, but the department did not disconnect the affected systems until over the weekend, according to federal technology information website nextgov.com. It said there was abnormal activity in the email system as recently as late October. The State Department breach follows similar intrusions disclosed in recent months at the White House, the Office of Personnel Management and, just last week, U.S. Postal Service and National Oceanic and Atmospheric Administration. USPS said it was the victim of an intrusion that may have compromised the personal information of more than 800,000 employees, as well as data on customers who contacted its call center during the first eight months of this year. In the NOAA case, four of the agency's websites were affected. The State Department cyberattack was first reported Sunday by The Associated Press. To read more click **HERE**

US State Department network shut amid reports of cyber breach

AFP, 17 Nov 2014 - The US State Department had to shut down its unclassified computer network over the weekend after hacking was suspected, the US media reported late Sunday. The State Department said in an email late Friday that the shutdown comes as scheduled routine maintenance to its main unclassified network, and would impact email traffic and access to public websites. But on Sunday reports emerged that there was evidence a hacker may have breached the security in portions of the system handling non-classified emails. A senior official told the Washington Post there had been "activity of concern" but that none of the department's classified systems had been compromised. If hacked, the State Department would be the latest in a series of government agencies to face cyber security breaches -- though it is not clear if there is any link between the incidents. Last week, the US Postal Service said hackers stole sensitive personal information from its employees in a large data breach this year, and got some customer data as well. A USPS spokesman said the breach affected as many as 800,000 people who are paid by the agency, including employees and private contractors. The statement said hackers also penetrated payment systems at post offices and online where customers pay for services. The agency was working with the FBI and other law enforcement in an investigation. And last month, the White House reported an intrusion in its unclassified computer network. In the course of addressing the breach, some White House users were temporarily disconnected from the network, an official said, but the computers and systems were not damaged. The Washington Post quoted sources as saying hackers believed to be working for the Russian government were believed to be responsible. To read more click **HERE**

Scotland Yard wages war on 200 cybercrime gangs in London
Standard.Co.Uk, 17 Nov 2014: Scotland Yard is battling more than 200 organized crime groups engaged in cyber fraud in London, police revealed today. A new Met cyber taskforce is investigating plots ranging from online dating fraud to mortgage scams involving million pound properties. Police say they are facing an overwhelming caseload of around 54,000 reports of cyber fraud in the capital each year – but admit the crime is still hugely under-reported. Detective Chief Superintendent Jayne Snelgrove, the head of the Met's new cybercrime and fraud unit codenamed Falcon, said officers were in the early stages of around 18 investigations. These ranged from online retail and auction site frauds to courier scams and investment frauds. So far, the squad – which was launched in October - has made more than 100 arrests and detectives were targeting a number of organized crime groups engaged in cyber fraud. Police believe more than 200 gangs from around the world are targeting London using the Internet, though the figure changes constantly. DCS Snelgrove says many gangs are operating in different countries and a number of Falcon's inquiries span the United States, parts of Europe and Russia. However, many of the cyber frauds are committed by home grown gangs or individuals. Around 54,000 reports of fraud were recorded by Action Fraud in London last year. To read more click **HERE**

Majority of UK Firms Would Hire Ex-Cons as Cyber-Security Pros
Infosecurity Magazine, 16 Nov 2014: Over half of senior IT and HR professionals would consider hiring former hackers in a bid to overcome crippling cyber-security skills gaps and shortages, according to new research from consultancy KPMG. The firm interviewed staff in UK businesses with anything from 500-10,000 employees and found increasing levels of concern when it comes to human resources, with three-quarters (74%) admitting new skills are needed to combat ever-evolving threats. However, despite the majority (60%) claiming to have a strategy to deal with any gaps that might arise, 57% said they are finding it more difficult to retain those highly skilled in specific areas of information security, and complained of high churn thanks to aggressive headhunting. With this backdrop, it's perhaps not surprising that 53% said they would hire a hacker to bring extra skills into the cyber-security team, while 52% said they would consider employing an expert even if they had a criminal record. The majority of those interviewed (57%) said it has become more difficult to retain skilled information security specialists over the past two years. Skills particularly in demand include data protection and privacy, which 70% of respondents admitted a shortfall in. A further 60% said they were having trouble finding candidates who could communicate effectively with the business – a perennial problem in the cyber-security sector. Serena Gonsalves-Fersch, head of KPMG's Cyber Security Academy, argued that firms would be better off developing cyber security skills within "current security and IT frameworks" than considering hires which may introduce greater risk into the organization. "With many businesses struggling to recruit cyber specialists and with their salaries increasing rapidly it has become less of an alien concept to considering tapping into the market of former hackers," she told Infosecurity. "Many of these people who have been behind cyber-crimes have the ability to identify potential threats and help companies mitigate cyber risk. This doesn't come without risk, but companies should have advanced enough identity and access management processes to not allow one employee to run the entire cyber security function."
[NMCIWG Note: Access to CUI/FOUO requires an individual to possess a security clearance of SECRET or higher – a convicted felon is unlikely to qualify for that clearance level] To read more click **HERE**

November 14, Softpedia – (International) **Personal info on more than 70,000 posted online by debt sellers.** The U.S. Federal Trade Commission (FTC) filed a complaint against debt collection companies Cornerstone and Company, LLC of Riverside, California, and Bayview Solutions, LLC, of St. Petersburg, Florida, for allegedly leaving the personally identifiable information (PII) of over 70,000 customers online on a publicly accessible Web site. The FTC stated that the Excel spreadsheets included bank account numbers, payment card numbers, debt amounts, dates of birth, and other information and that the files were downloaded more than 500 times. Source: http://news.softpedia.com/news/Personal-Info-on-More-than-70-000-Posted-Online-By-Debt-Sellers-464909.shtml

November 14, Securityweek – (International) **OnionDuke APT malware distributed via malicious Tor exit node.** Researchers with F-Secure identified a piece of sophisticated malware dubbed OnionDuke that was distributed by a Russia-based Tor exit node and uses the same command and control infrastructure as the MiniDuke malware used in advanced persistent threat (APT) campaigns. Source: http://www.securityweek.com/onionduke-apt-malware-distributed-malicious-tor-exit-node

November 13, Threatpost – (International) **Internet voting hack alters PDF ballots in transmission.** Researchers at Galois published a paper demonstrating how an attacker could conduct an attack against home routers by altering the router firmware that would allow them to intercept a PDF voting ballot and modify it before sending it to the election authority. Source: http://threatpost.com/internet-voting-hack-alters-pdf-ballots-in-transmission/109333

November 12, Associated Press – (National) **US confirms climate agency websites hacked.** A National Oceanic and Atmospheric Agency spokesman confirmed November 12 that four of its Web sites were compromised by an Internet-sourced attack after staff detected the intrusion and began incident response efforts. The agency performed unscheduled maintenance and all services were fully restored. Source: http://www.bostonherald.com/news_opinion/national/2014/11/us_confirms_climate_agency_websites_hacked

Steam Password Stealer Is Stored on Google Drive

Softpedia, 17 Nov 2014: A piece of malware aimed at stealing Steam account credentials has been making the rounds targeting gamers through the platform's chat client for at least a week, being delivered from a Google Drive account that is still active. It's no secret that the vigilance of gamers on Steam is constantly tested by luring them to click on malicious links posted in the chat box. Some users are quick at spotting the attack and stay away from the URLs, but others do fall victim to such attempts and end up with their Steam account being hijacked. An obvious scam can still make some victims The scam is quite simple and it is encountered on Steam more often than one would like. A gamer known as Onyx showed in an entry on Tumblr the standard approach used by the attackers: a simple message claiming to be from someone known to the potential victim entices to click on a link (oftentimes shortened) under the pretext to find more info about the alleged friend. The URL in fact leads to malware, which, once installed on the system, steals the log-in data for the Steam account, according to Bart Blaze, malware researcher at Panda Security, who analyzed the sample and provided a technical overview in a blog post on Sunday. Blaze explains that the malicious link proceeds to download a screensaver file (SCR), which is an executable, from Google Drive; the SCR purports to be a picture and even has an image as the file icon. "Note that normally, the Google Drive Viewer application will be shown and this will allow you to download the .scr file. In this case, the string '&confirm=no_antivirus' is added to the link, which means the file will pop-up immediately asking what to do: Run or Save. (and in some cases download automatically)," he writes. The file has been reported by the researcher on Sunday, but it appears that no action has been taken against it by now because it is still available in the Google cloud. Luckily, most reputable antivirus solutions detect it and prevent its download on the computer. 37 out of 55 antivirus engines on VirusTotal have no trouble quarantining it on the spot. In the researcher's analysis, it is noted that the malware connects to a server hosted in the Czech Republic, where the stolen information is probably uploaded. Signs of the Steam account log-in information compromised via this threat consists in the presence of a process named "temp.exe," "wrrrrrrrrrrr.exe," "vv.exe," or one with a random name running on the system; this can be checked with Task Manager. In case of compromise, users are recommended to immediately change the password for the Steam account and scan the system with a reputable antivirus. To read more click **HERE**

HSBC Bank in Turkey Hacked, Card Fraud Risk Not Present

Softpedia, 16 Nov 2014: A cyber-attack on the computer systems of the HSBC Bank in Turkey has compromised card information of customers, but officials say that the intruders cannot use the data for fraudulent transactions. Detected in the past week through internal verification mechanisms, the incident resulted in exposing card data consisting of number, expiry date and owner's name. The account numbers associated with the cards have also been compromised. In a FAQ explaining the details of the breach, the bank says that despite the fact that the attacker(s) managed to access this information, there is no risk of card fraud, neither through cloning the cards nor through online transactions. Printing fake cards and withdrawing money from ATMs or using them at retail shops is not possible simply because there is insufficient data (magnetic strip information and PIN code is not available) to pull this type of fraud. In the case of online shopping, which requires less information from the customer, the bank does not clearly state why fraudulent transactions cannot be carried out, but one reason is the absence of the card security code (CVV) from the list of compromised information. A CVV (Card Verification Value), or CVC (Card Verification Code) usually consists of the last three numbers printed on the back of the card. Some banks issue a four-digit CVV and it is present on the front of the card. These verification codes are required for each online shopping session to prove that the buyer actually has the card with them and the data has not been stolen from a database; storing CVVs on merchants' systems is against the Payment Card Industry Data Security Standard (PCI DSS). On the other hand, some retailers do not ask for this security code in order to complete a purchase. This happens in the case of micropayments, which are limited to a specific amount. Merchants supporting these transactions are doing it in an effort to make the entire purchase process easier for their customers. Moreover, it has been shown that clients are more willing to make small purchases. With micropayments, if the card data (save for the CVV) is already present in the shopping cart database, the card verification code is no longer required to complete the order. If fraudulent transactions occur, they are obviously willing to accept them and to reimburse the customer, since the process was not properly secured on their end. Although the risk of fraud is non-existent in theory, HSBC officials said that the bank's clients would not be held liable for any illegal payment occurring as a result of the attack on their systems. For the time being, the bank has not found any evidence of suspicious activity on the accounts of the affected individuals, but said that it is confident that the attack has no financial risk. With regards to the amount of records exposed, various online sources report a number of about 2.7 million. To prevent a similar incident from repeating, the bank has proceeded to upgrade the security measures. An investigation has been initiated in order to learn the identity of the attacker(s). To read more click **HERE**

Suspects Tied to WireLurker Malware Arrested in China

Softpedia, 15 Nov 2014: The Beijing Municipal Public Security Bureau has arrested three individuals for involvement in the creation and distribution of WireLurker malware that compromises iOS devices and made hundreds of thousands of victims in China. The three suspects were identified based on information received from security company Qihoo 360 Technology. In a post on Sina Weibo, the Bejing police announced that the three suspects, identified only by their surname (Chen, Lee and Wang), have been taken into custody on Thursday for conspiring to write malicious software used for illegal profits. WireLurker would be spread through the Maiyadi store for OS X applications, which hosted premium pirated content. A report from AlienVault researcher warned that a version for Windows was also in use. According to researchers from Palo Alto Networks, who discovered the malware and published their findings last week, the cybercriminals infected popular programs and uploaded them to the online repository. During their analysis they found 467 pieces of trojanized gaming software. After installation on the system, WireLurker would wait for an iOS device to connect to the computer (OS X or Windows) to compromise it. The malicious apps that would then be downloaded to the desktop computer and upon detecting a USB-connected iOS device, they would be sent to the target. The location hosting the malicious apps has been identified at the 124.248.245.78 IP address. The malware works regardless if the device is jailbroken or not because it also included apps signed with an enterprise digital certificate; these are not passed through the rigorous security checks from Apple, like the items in the official store,

because they are believed to be trustable since certificates are issued to verified organizations for building proprietary software for use in corporate environment. The report from the Beijing police on the Chinese microblogging platform is brief, but it does inform that the Maiyadi iOS store has been shut down. WireLurker collects the product serial and model numbers, phone number, Apple ID, Wi-Fi address, disk usage, and the unique device identifier – UDID. The purpose it has been built for is unclear because, despite the ability to steal large amounts of information, this does not point to a specific motive, the Palo Alto Networks said in their report. To protect its customers, Apple started to block the malicious apps in the Maiyadi third-party store immediately after hearing the news about WireLurker. To read more click **HERE**

New Encryption Ransomware Offers File Decryption Trial

Softpedia, 15 Nov 2014: Cybercriminals have adapted their ransomware game to a more user-friendly variant of crypto-malware to get the victims pay the unlock fee and even included a trial for the file decryption feature. Dubbed CoinVault (no connection with the legitimate coin exchange services online), the threat has an interface with all the functions necessary for viewing the locked data, paying the ransom and initiating the decryption mechanism based on the key provided after the payment is recorded. It is clear that the malware authors tried to make the entire scam as simple a process as possible for the user. They even added a button for copying the bitcoin wallet address and a 24-hour countdown timer that lets the victim know how much time they have to pay the ransom until it increases. Researchers at Webroot discovered the new variant on Friday and tested the decryption functions, which, as it was expected, worked. The algorithm used for locking up the data is the AES-256, a rudimentary one compared to what other cryptomalware families rely on; however, this does not make CoinVault any less dangerous. CryptoWall relies on asymmetric encryption, which requires two keys (public – for encryption, and private, derived from the public one – for decryption) to secure the information; only the holder of the private key can decrypt the files. By contrast, AES-256 is a symmetric encryption algorithm that relies on a single key for both encrypting and decrypting, 256-bit in length; find that key and the data is freed. CryptoWall is one of the most prominent representatives of the ransomware malware with encryption capabilities. It currently has more than 80 variants in the wild and it made hundreds of thousands of victims worldwide, with cybercriminals making more than $1.1 million / €878,000 this year. According to CoinVault's description, the AES key is stored on a server that releases it to the victim as soon as the ransom is paid. A similar piece of crypto-malware has been discovered by researchers at iSight Partners back in August. They named it TorrentLocker and the same AES algorithm was used; moreover, it included decryption testing, too. The purpose of offering the victims the possibility to try out the unlocking mechanism is to instill confidence that the data is released once the payment is accepted. Having an updated antivirus solution installed on the computer can sometimes be enough to prevent crypto-malware from taking the files hostage, but the best solution is to have a backup of the important data ready. This type of threat does nothing but encrypt the files; if a safecopy exists, it can be restored at no financial cost for the user. To read more click **HERE**

ShadowCrew Member Gets Nine Years in Jail, Ordered to Pay $50 Million

Softpedia, 14 Nov 2014: A 28-year-old man from Augusta, Georgia, was sentenced on Thursday to 115 months in a federal prison for buying stolen credit card data and personal information through an underground carding forum. He was also ordered by the court to pay $50.8 million in restitution. Identified as Cameron Harrison, the cybercrook pleaded guilty at a court hearing in April, admitting his association with an underground marketplace for trading identity theft and credit card fraud information known as Carder.su; the forum was also involved in money laundering, narcotics trafficking and computer crimes. Harrison used the alias "Kilobit" in the online environment and was identified after purchasing a fake driver's license from an undercover agent through the Carder.su network. That was when he said that he had been part of the ShadowCrew group that engaged in cyber fraud activities between 2002 and 2004. In an action dubbed Operation Open Market in October 2012, the US Immigration and Customs Enforcement's Homeland Security Investigations (ICE HSI) and the US Secret Service cooperated to bring

down the Carder.su forum. As a result, 55 people have been charged. According to a statement from the Department of Justice, "26 individuals have been convicted and the rest are either fugitives or are pending trial." Carder.su united a closed group of individuals, who tried to carry out their activities under the radar, taking safety measures such as communicating through encrypted channels. Getting into the group required the recommendation of two current members. This is far from being an uncommon practice in the case of cybercriminal organizations. At the time of his arrest, Harrison had more than 260 stolen credit and debit card number stored on his laptop and in email accounts. US Assistant Attorney General Leslie Caldwell said that the crook lived off the stolen cards. "This significant sentence is entirely fitting given that this defendant's actions and those of the larger criminal organization harmed countless innocent Americans and seriously compromised our financial system," said Peter T. Edge, HSI Executive Associate Director. US Attorney Daniel Bogden added in a communication that Carder.su was responsible for thieving more than $50 million from identity theft victims, who suffered both financially and emotionally. Putting Harrison behind bars is definitely a victory for the justice system, and the sentence he received comes as a warning for other individuals involved in highly lucrative illegal businesses such as ShadowCrew and Carder.su. To read more click **HERE**

Sheriff's Office Pays Ransom to Unlock Files Encrypted by CryptoWall

Softpedia, 14 Nov 2014: A computer system of the Sheriff's Office in Dickson County, Tennessee, has been hit by the CryptoWall ransomware, locking access to thousands of files. The incident occurred in late October, when someone in the office clicked on a malicious advertisement placed on the website of a local radio station and triggered a drive-by download attack with the crypto-malware as the payload. As soon as the malware reached the computer, it started to encrypt files with certain extensions and demanded the owner to pay a ransom for getting the data back. Since no backup mechanism was in place for that particular workstation, the IT director of the office, detective Jeff McCliss, was faced with a dire situation, where either the fee was paid or the data remained locked. The detective opted for the first choice and delivered the $500 requested by the attackers in digital currency. The decision was taken after consulting with higher law enforcement organizations that participated in the investigation of the event, such as the Tennessee and the Federal Bureau of Investigation. According to Channel 5 News, they all agreed that the only chance to get the data back was to cough up the money. "Every sort of document that you could develop in an investigation was in that folder. There was a total of 72,000 files," he told the news station. The information encrypted by the malware included important case files, like autopsy reports, witness statements, and crime scene photographs. Without these, criminal investigations would have been halted and evidence would have disappeared. Security experts strongly recommend victims of ransomware not to pay the money, firstly because there is no guarantee that the crooks will keep their end of the bargain, and secondly, to discourage the phenomenon; with victims not paying up, the cybercriminals would be less inclined to carry out this sort of attack. However, the same security experts also recommend that a backup system be in place, and in the case of a police organization, one would think that there are plenty of reasons to protect information from all sorts of threats, be they malware or just hardware malfunctions. "Is it better to take a stand and lose all that information? Or make the payment grit your teeth and just do it?" he said. "It made me sick to have to do that;" hopefully sick enough to set up a backup mechanism, especially since the office was lucky enough to have to deal with crooks who still value their word and delivered on their promise to provide the decryption key in exchange for the money. This is not the first time CryptoWall infects the computers of a police station. In June, the same malware family held hostage the data on a system of the police department in Durham, New Hampshire. Fortunately, the officers there were much better prepared and had a backup solution in place, which allowed them to restore all the data and continue focusing on the ongoing criminal investigations. To read more click **HERE**