The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

10 March 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

March 6, Los Angeles Times – (California) **Computers with L.A. County patients' personal data are stolen.** Los Angeles County officials reported March 6 that 8 computers and 2 monitors were stolen after a Torrance office of Sutherland Healthcare Solutions, which handles billing and collections for the county's Department of Health and Human Services and Department of Public Health, was burglarized February 5. The equipment included personal data and billing information for nearly 168,500 patients of county medical facilities. Source: http://www.latimes.com/local/la-me-patient-data-stolen-20140307,0,1463656.story#axzz2vHscBlwc

March 7, Help Net Security – (International) **Siesta cyber espionage campaign targets many industries.** Researchers at Trend Micro discovered a cyberespionage campaign dubbed Siesta that is targeting several industries, including energy, financial services, healthcare, and defense. The campaign uses malware that enters dormancy at regular intervals and when active, sends out spoofed emails to various companies containing a malicious link that drops both a legitimate .pdf file and a malicious executable file. Source: http://www.net-security.org/secworld.php?id=16490

March 7, Softpedia – (International) **Over 40 bugs, including 4 security vulnerabilities, fixed in Joomla 3.2.3.** The newest version of Joomla, Joomla 3.2.3, was released for download, closing four security vulnerabilities. Users were advised to update their installations immediately. Source: http://news.softpedia.com/news/Over-40-Bugs-Including-4-Security-Vulnerabilities-Fixed-in-Joomla-3-2-3-431030.shtml

March 7, The Register – (International) **comiXology's Phantom Zone breached by villainous Haxxor.** E-comics service comiXology informed customers that attackers had breached its systems and accessed a database containing usernames, email addresses, and encrypted passwords. All customers were required to change their passwords as a precaution. Source: http://www.theregister.co.uk/2014/03/07/comixologys_phantom_zone_breached_by_evil_haxxor/

March 6, SC Magazine – (International) **'Dendroid' RAT trojanizes apps, enables compromise of Android devices.** A researcher at Symantec reported discovering a new HTTPS remote access trojan (RAT) dubbed Dendroid for sale on underweb marketplaces. Dendroid allows attackers to add malicious code to legitimate Android apps in order to gain remote access to infected devices. Source: http://www.scmagazine.com/dendroid-rat-trojanizes-apps-enables-compromise-of-android-devices/article/337191/

Hackers dox Mt. Gox CEO, say they have proof of fraud
Heise Security, 10 Mar 2014: News about what actually happened in the days leading up to the Mt. Gox Bitcoin exchange filing for bankruptcy are few and far between, and some of its customers are losing their patience, especially when there is no record in the Bitcoin blockchain of the allegedly stolen 850,000 bitcoins moving. Yomiuri Shimbun sources confirmed that Mt. Gox was hit by a massive DDoS attack that was separate from the attacks aimed at stealing

bitcoins via malformed transactions. The DDoS attacks came prevalently from servers in the US and Europe. Also this weekend hackers compromised the official blog and the Reddit account of Mt. Gox CEO Mark Karpeles, as well as some of the company's servers. "It's time that MTGOX got the bitcoin communities wrath instead of Bitcoin Community getting Goxed. This release would have been sooner, but in spirit of responsible disclosure and making sure all of ducks were in a row, it took a few days longer than would have liked to verify the data," they wrote in a message on Karpeles' blog, and offered a link to a 716 Mb archive containing "relevant database dumps, csv exports, specialized tools, and some highlighted summaries compiled from data," but no user database dumps. According to Forbes, the file "appears to include an Excel spreadsheet of over a million trades, a file that purports to show the company's balances in eighteen difference currencies, the backoffice application for some sort of administrative access to the databases of Mt. Gox's parent company Tibanne Limited, a screenshot of the hackers' access to those databases, a list of Mark Karpeles' home addresses and Karpeles' personal CV." "In the hackers' summary of Mt. Gox's balances in various currencies, they point to a claimed balance of 951,116 bitcoins, which they take as evidence that Mark Karpeles' claim to have lost users' digital currency to hackers is fraudulent," added Forbes' Andy Greenberg, but pointed out that is not evidence of Karpeles' involvement in the apparent theft. He also noted that a user on the BitcoinTalk forum apparently tried to sell the Mt. Gox user database, complete with real names and passport scans, but whether he or she actually had the dump in question has not been confirmed. To read more click **HERE**

Personal info of 12 million KT customers stolen and misused

Heise Security, 7 Mar 2014: Two men have been arrested in connection with the massive KT Corp. data breach that resulted in the theft of personal and financial information of some 12 million customers of the South Korean telecom giant. According to the CNN, one of the arrested men, a 29-year-old surnamed Kim, was a hacker who broke into the company's computer system with customized hacking software and extracted customer information such as names, resident registration numbers and bank account information. The initial breach apparently happened in February 2013, and he has been extracting the data ever since. He allegedly sold it to a 37-year-old man surnamed Park, a telemarketing business owner that used the information to credibly impersonate a KT Corp. employee in order to sell cell phones. Another man has been arrested but almost immediately released. Apparently, in the last year, they managed to earn themselves nearly $11 million through this scheme. The South Korean Ministry of Science, ICT and Future Planning is warning potentially affected users to be on the lookout for phishing emails impersonating the company and taking advantage of the situation to make them share more personal details. To read more click **HERE**

Using free Wi-Fi in Europe is risky

Heise Security, 7 Mar 2014: Internet users would do well to be extra careful when attempting to use public Wi-Fi hotspots in Europe, as hackers and cyber crooks have lately ramped up their efforts to steal personal and financial data sent over these unsecure networks. The warning comes from Troels Oerting, the head of Europol's cybercrime center, who says that the law enforcement agencies are helping several European countries in the aftermath of these type of attacks. "We should teach users that they should not address sensitive information while being on an open insecure Wi-Fi internet," he pointed out for the BBC. "They should do this from home where they know actually the Wi-Fi and its security." Oerting says that the attackers aren't inventing new attack techniques, but are using old, tried and true ones that still obviously work: they usually set up fake hotspots with a name (SSID) similar the one set up by coffee shops, stores, hotels, libraries and other public establishments. Once users connect to it and start using it, all information they send out is captured by the criminals. There are a number of things you can do and precautions you can take to make sure that you are as safe as you can be while using public Wi-Fi networks. Avoid accessing services such as online banking, ePayment services or any site that stores payment information via open public Wi-Fi. If you simply must do some online banking, use your mobile data plan with your bank's mobile app. To read more click **HERE**

HTTPS can't be trusted to obscure private online activity

Heise Security, 6 Mar 2014: HTTPS was initially used to prove to Internet users that the website and web server with which they are communicating are indeed the ones they want to communicate with, but later this use was extended to keeping user communication, identity and web browsing private. But a group of researchers has, unfortunately, proven that HTTPS is a lousy privacy tool, and that anyone who can view, record and analyze visitors' traffic can identify - with 89 percent accuracy - the pages they have visited and the personal details they have shared. The group consisting of researchers from UC Berkley and Intel Labs has captured visitors' traffic to ten popular healthcare (Mayo Clinic, Planned Parenthood, Kaiser Permanente), finance (Wells Fargo, Bank of America, Vanguard), legal services (ACLU, Legal Zoom) and streaming video (Netflix, YouTube) websites. "Our attack applies clustering techniques to identify patterns in traffic. We then use a Gaussian distribution to determine similarity to each cluster and map traffic samples into a fixed width representation compatible with a wide range of machine learning techniques. Due to similarity with the Bag-of-Words approach to document classification, we refer to our technique as Bag-of-Gaussians (BoG)," they explained in a whitepaper. "This approach allows us to identify specific pages within a website, even when the pages have similar structures and shared resources." Depending on which websites they interact with, this type of attack can have many consequences for Internet users as details such as medical conditions they have or medical procedures they have or are thinking of having might be revealed, legal problems they have and actions they might take might be shown, and financial products they use and videos they watch might point to information they would like to be kept hidden from anyone but themselves. Who can leverage such an attack? Well, anyone who has access to those web pages and can capture the victims' traffic - in practice this means ISPs (whether working for the government or not), employers monitoring online activity of their employees, and intelligence agencies. Fortunately, they have thought of several defense techniques which, if implemented, can drastically reduce the accuracy of such an attack. Also, they pointed out, there are other things that can affect the attack's effectiveness. "To date, all approaches have assumed that the victim browses the web in a single tab and that successive page loads can be easily delineated. Future work should investigate actual user practice in these areas and impact on analysis results. For example, while many users have multiple tabs open at the same time, it is unclear how much traffic a tab generates once a page is done loading. Additionally, we do not know how easily traffic from separate page loadings may be delineated given a contiguous stream of user traffic," they noted. "Lastly, our work assumes that the victim actually adheres to the link structure of the website. In practice, it may be possible to accommodate users who do not adhere to the link structure." To read more click **HERE**

A peek into China's burgeoning mobile cybercriminal underground

Heise Security, 6 Mar 2014: Every country's cybercriminal underground market has distinct characteristics, and with 500 million national mobile Internet users and the number continuously rising, the Chinese underground market is awash with cyber crooks buying and selling services and devices aimed at taking advantage of them. Trend Micro's senior threat researchers Lion Gu has been scouring forums, online shops and QQ chats to give us a sense of what is actually going on this burgeoning mobile underground. Mobile apps that stealthily subscribe users to premium services are, naturally, very popular with cyber crooks in China as in the rest of the world. Premium service numbers can also be bought on underground markets. Network carriers usually assign premium service numbers to qualified service providers, but obviously some of them are not adverse of selling them on to criminals. Another type of malicious SMS-sending apps is the so-called SMS forwarders - apps that intercept text messages carrying sensitive data and forward it to the crooks. These messages include those with reset passwords, verification codes, etc. "Like premium service abusers, they also delete the text messages they intercept to hide traces of infection. If cybercriminals get hold of victims' usernames in certain sites, they can easily change passwords and take control of stolen accounts," Gu points out. Next are SMS and iMessage spamming software and associated devices. This type of spam usually delivers unwanted and pricy offers of goods and services, as well leads users to sites hosting malware or phishing forms. To send out spam messages in huge numbers, the crooks can buy and use a number of different devices. GSM modems can both send and receive text messages, and they function as a normal mobile phone. Just insert a SIM card (or more) and you

can get cracking. Just go give you an idea: a 16-slot (with a SIM card in each) GSM modem can send 9,600 text messages per hour. Internet short message gateways can do it even faster. These devices are usually provided to service providers by mobile network carriers, but can obviously be misused by cyber scammers as well. An SMS server - also known as "fake base station" - is radio frequency hardware that can send out software-defined radio signals in GSM frequency ranges. "When running, an SMS server announces itself as a base station by sending a high-power signal, which forces all nearby mobile phones to disconnect from the legitimate base stations of their network carriers and instead connect to the SMS server. The SMS server can then push out spam to the mobile phones," Gu explains. "When finished, the SMS server disconnects from the mobile phones, which are then reconnected to their legitimate base stations." iMessage spam computer software finds phone numbers tied to Apple devices and sends messages to it. Phone-number-scanning services are also popular with SMS spammers that don't want to waste their time and effort by sending out spam to numbers that are temporarily or no longer in use. Finally, there are services that offer to boost the rank of malicious apps on third-party app stores, which are dominant in China. All of these devices and service come at a price, and you can check out the typical price lists in Gu's whitepaper (**LINK**). To read more click **HERE**

Statista Says Around 50,000 Users Are Impacted by Data Breach

SoftPedia, 10 Mar 2014: On Saturday, we learned that statistics company Statista suffered a data breach. The company has responded to my inquiry about the incident and provided additional details. It turns out that roughly 50,000 users are impacted by the data breach. The incident was discovered after spam emails started landing in email addresses that have been used by the company only internally. After the spam emails were spotted, the company reviewed its systems and discovered the intrusion, Statista representatives told me in an emailed statement. Shortly after discovering the breach, the company started sending out notifications to alert customers. "According to an internal assessment and that of external IT professionals the password data cannot be used by third parties due to masking procedures. Of course, you can still change your assigned password at any time in your profile if you wish," Statista wrote in those emails. However, it turns out that they should have reset passwords or ask customers to change them. The statement about "masking procedures" is misleading. The company's representatives say that since the relaunch in December 2013, they've been using "512-bit encryption with salt." However, the passwords of those who signed up before this date were stored in the Statista database as MD5 hashes. As many experts will tell you, MD5 passwords can be easily cracked. If you're a Statista customer and you're reading this, you should change your password immediately. If you've used the same password for multiple online services, change the other ones as well. Also, since Statista has been getting spam emails, it's likely that all of the 50,000 users whose email addresses have been exposed are receiving unsolicited emails. Users should act with caution if they come across suspicious emails in their inbox. To read more click **HERE**

Justin Bieber's Twitter Hacked, Fans Lured to Shady Website

SoftPedia, 10 Mar 2014: Over the weekend, cybercriminals managed to hijack Justin Bieber's 50 million follower Twitter account. The attackers used the compromised account to lure the pop artist's fans to a website offering Twitter followers and other similar services. The spam tweets were written in Indonesian and included shortened links. The links pointed to a website called rumahfollowers(dot)tk. This site is no longer accessible, but it appears to be a service that offers Instagram and Twitter followers and Facebook likes. The tweets have been removed by Justin Bieber's team. The celebrity posted the following message on Twitter after cleaning up his feed: "all good now. we handled it." Some of his fans believe the spammers hijacked his account after tricking him into clicking on a link. This is a plausible scenario, since that's how most Twitter accounts are compromised. The attackers trick victims into handing over their credentials on a phishing site, or have targeted users install an app that allows the cybercrooks to post messages. 50 million followers means that a lot of people might have clicked on the links. If you're one of them, you should change your password and revoke access to all suspicious apps to make sure the scammers can't abuse your account. This isn't

the first time Justin Bieber's Twitter is hacked. However, it appears that the artist still has a few things to learn about online security. To read more click **HERE**

Classified Military Files Possibly Stolen in India Defense Ministry Hack

SoftPedia, 10 Mar 2014: In December 2013, around 50 computers belonging to India's Defense Ministry and the country's Defence Research and Development Organisation (DRDO) were hacked. The attackers might have gained access to classified information. According to the Times of India, the breach was discovered by intelligence agencies. They've found a piece of spyware capable of retrieving files even from devices that are not connected to the Internet. The penetrated computers are located in the Secretariat Building in New Delhi, which houses some of the most important ministries of the Cabinet of India. The Secretariat has two blocks of symmetrical buildings called the North Block and the South Block. The targeted devices are in the South Block and they're said to belong to the Army and two other forces. Sources have told the Times of India that as many as 30 classified files might have been accessed by the hackers. Officials say they're investigating the incident, but they've downplayed the seriousness of the breach. On the other hand, after the breach came to light, an advisory was published regarding the separation of computers that store confidential information from ones connected to the public Web. China and Pakistan are believed to be behind many cyber espionage operations targeting India, but it's uncertain who is responsible for this particular attack. To read more click **HERE**

Hackers Hijack Blog of Mt. Gox CEO, Accuse Him of Lying to Customers

SoftPedia, 10 Mar 2014: On Sunday, hackers breached the official blog of Mark Karpeles, the CEO of the Bitcoin exchange Mt. Gox. After gaining access to balances, the hackers have determined that Karpeles lied to customers when he said that their Bitcoins had been stolen. The hackers have published a post on Karpeles' blog, along with links to stolen information. The post added by the attackers has been removed, but it's still available via Google's cache. "It's time that MTGOX got the bitcoin communities wrath instead of Bitcoin Community getting Goxed. This release would have been sooner, but in spirit of responsible disclosure and making sure all of ducks were in a row, it took a few days longer than would have liked to verify the data," the hackers wrote. They haven't leaked any user data because they only want to get back at the Bitcoin exchange service, not its customers. However, they have published what appears to be a file containing Bitcoin transactions, a CV of Karpeles, some applications used by Mt. Gox, and a screenshot to demonstrate that they've gained access to the company's databases. The information is contained in a 716 Mb archive file. On one hand, the hackers say they haven't stolen any Bitcoins because there "were not to steal." On the other hand, they've published balances for various currencies. Next to the BTC balance, which shows 951,116 Bitcoins, the hackers wrote, "That fat [expletive] has been lying!" Forbes highlights that the information leaked by the hackers doesn't necessarily demonstrate that Mt. Gox has been lying to customers about their coins being stolen. It could simply mean that the exchange's accounting shows the Bitcoins before being stolen. Mt. Gox claims to have lost a total of 850,000 Bitcoins, 750,000 of which belonging to customers. However, experts say they haven't seen the coins being moved. At the beginning of March, we reported that hackers claimed to have breached Mt. Gox's systems in an effort to find out what happened. At the time, a user with the online moniker "nanashi____" leaked a conversation between Karpeles and a Japanese banker, and some Mt. Gox staff information. In a post published on Bitcoin Talk on Sunday, nanashi offered to sell 20 Gb of data allegedly stolen from Mt. Gox. He asked for 100BTC for the data. "Selling it one or two times to make up personal loses from gox closure," nanashi wrote. Bitcoin Talk has removed the post, but it can still be viewed through Google's cache. To read more click **HERE**

Neutrino Exploit Kit Reportedly Put Up for Sale by Its Author [Updated]

SoftPedia, 3 Mar 2014: The author of the Neutrino exploit kit has reportedly decided to sell his creation. The reason: he says he doesn't have time to deal with customer support, accepting payments and the other activities that come with the territory. The self-proclaimed security researcher Trojan7Sec has contacted the author of the exploit kit and learned

that Neutrino brings him a monthly profit that ranges between $30,000 (€21,800) and $60,000 (€43,600). The exploit kit is allegedly being sold for $34,000 (€26,700). The price includes the existing client base. Trojan7Sec believes that while Neutrino is a good exploit kit, the client database is most likely the bulk value of the price tag. The expert has told me that, based on his calculations, the number of customers is in the 66-132 range. "The quality of the EK depends on the coder. If someone buys it they could add another 10 exploits and make it the best," Trojan7Sec noted. The administration of servers and domains costs around $3,000 (€2,180) per month. Trojan7Sec has been monitoring live Neutrino domains and found that their number has dropped right now. However, the expert says this is not out of the ordinary. The existence of the Neutrino exploit kit was first revealed by the security researcher Kafeine. Initially, it was designed to exploit a couple of Java vulnerabilities: CVE-2013-0431 and CVE-2012-1723. At least one other exploit was added later on. Neutrino has been rented to cybercriminals on a shared server for $150 (€108) per week or $450 (€324) per month. However, after the arrest of Paunch, the developer of the notorious BlackHole exploit kit, the author of Neutrino announced some drastic pricing changes, asking $1 million (€730,000) per month from customers who didn't speak Russian. Update. Some of our readers highlight the fact that Trojan7Sec is not the most trustworthy source. However, a reputable researcher who wishes not to be named has confirmed that Neutrino is being sold. He couldn't confirm the price tag. To read more click **HERE**