The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

18 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

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, Sandia Labs

Distribution
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings Credit is given to the NMCIWG for the compilation of open source data

March 14, Arizona Daily Star – (Arizona) **Stolen laptop from St. Mary's Hospital in Tucson contains patient information.** About 1,700 St. Mary's Hospital patients were notified after a laptop was stolen from a hospital work room, Hospitalists of Arizona officials stated March 14. Authorities are investigating and stated that the laptop contained prescription information and patients' personal information. Source: http://azstarnet.com/news/local/stolen-laptop-from-st-mary-s-hospital-in-tucson-contained/article_e9e32ed8-abea-11e3-87c9-001a4bcf887a.html

March 14, Glenwood Springs Post Independent – (Colorado) **Computer virus may have compromised Valley View Hospital patient information.** Valley View Hospital officials reported that the personal information of roughly 5,400 patients may have been compromised by a computer virus that infected the hospital's computer system. Authorities are investigating the incident, which was discovered in January, and have taken steps to quarantine the virus and determine if the data was improperly accessed or transmitted to an outside entity. Source: http://www.postindependent.com/news/10613337-113/information-hospital-personal-virus

March 17, Help Net Security – (International) **US announces transition of oversight over Internet's domain name system.** The U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) announced its intention to transition oversight of Internet domain name functions to global stakeholders. The NTIA requested that the Internet Corporation for Assigned Names and Numbers (ICANN) convene stakeholders and develop a transition proposal as a first step. Source: http://www.net-security.org/secworld.php?id=16530

March 17, Softpedia – (International) **Google addresses Chrome OS vulnerabilities presented at Pwnium 2014.** Google released an update to its Chrome OS browser-based operating system, closing seven vulnerabilities that were identified at the Pwnium 2014 competition the week of March 10. Source: http://news.softpedia.com/news/Google-Addresses-Chrome-OS-Vulnerabilities-Presented-at-Pwnium-2014-432533.shtml

March 16, The Register – (International) **iOS 7 has weak random number generator.** Researchers at Azimuth Security found that the random number generator used in the iOS 7 mobile operating system is weak to brute force attacks that could allow attackers to exploit vulnerabilities previously unable to be exploited. Source: http://www.theregister.co.uk/2014/03/16/ios_7_has_weak_random_number_generator/

Two Ukrainians and One American Charged for Role in Global Cybercrime Operation
SoftPedia, 18 Mar 2014: Three men have been charged with conspiracy to commit wire fraud, conspiracy to commit access device fraud and identity theft, and aggravated identity theft. They're believed to be part of an international cybercrime operation that targeted financial institutions and other major organizations in the Unites States. The suspects are 33 year old

Oleksiy Sharapka, 39-year-old Leonid Yanovitsky, both from Kiev, Ukraine, and Richard Gundersen, 47, a resident of Brooklyn, New York. They're accused of hacking into customer accounts at banks, brokerage firms, government agencies and payroll processing companies. They've attempted to steal at least $15 million (€10.7 million) from the US customers of various organizations. The list of targeted organizations includes Aon Hewitt, Citibank, E-Trade, Electronic Payments, Automatic Data Processing, JP Morgan Chase, Fundtech Holdings, iPayment, Ameritrade, PayPal, Nordstrom Bank, USAA, Veracity Payment Solutions, TIAA-CREF, and even the US Department of Defense's Defense Finance and Accounting Services. Once they gained access to bank accounts, the fraudsters transferred money from them to accounts and pre-paid debit cards they controlled. Later, the money was withdrawn from ATMs or the funds were used to make fraudulent purchases in various US states. In addition, they also used stolen identity information to file fraudulent tax returns with the IRS. The criminal proceeds were sent to the masterminds of the operation, who resided overseas, via wire transfer services. Sharapka, who is said to have directed the conspiracy, and Yanovitsky, who allegedly helped him, are fugitives. Gunderson is accused of facilitating the movement of criminal proceeds. The indictment reveals that Sharapka was the leader of a criminal enterprise called the "Sharapka Cash Out Organization," which operated between around March 2012 and around June 2013. Each of the suspects faces a maximum of 20 years in prison for the conspiracy to commit wire fraud charges, 5 years for the access device fraud and identity theft conspiracy count, and two years for the aggravated identity theft counts. They can also be ordered to pay massive fines. In June 2013, eight individuals – including Sharapka, Yanovitsky and Gunderson – were charged with conspiracy to commit wire fraud, conspiracy to commit money laundering and conspiracy to commit identity theft. Many of the suspects were arrested at the time by law enforcement. Gunderson and another suspect, Lamar Taylor, 37 were being pursued by authorities. Several US agencies have taken part in the investigation, including the US Secret Service, the ICE, the DOD's Criminal Investigative Service, and the IRS. To read more click **HERE**

Australian AG Wants to Make Refusing to Hand over Encryption Keys a Criminal Offense

SoftPedia, 18 Mar 2014: This week's threat to privacy comes from Australia and the main actor is none other than the country's Attorney General who wants new laws to force users and providers of encrypted Internet communication services to hand over the keys that would allow them to decode the data intercepted by authorities. According to ITNews, the proposal isn't plain as day, but rather got buried into a submission by the department to a Senate inquiry on revision of the Telecommunications Interception Act, as they hoped no one would find it. While the Attorney General's office fears that there are too many encrypted communications which make the intercepted data unreadable, the obvious problem is that privacy means nothing to them. Furthermore, they seem to find it irritating that more and more people adopt encryption to mess with authorities engaging into mass surveillance. "Sophisticated criminals and terrorists are exploiting encryption and related counter-interception techniques to frustrate law enforcement and security investigations, either by taking advantage of default-encrypted communications services or by adopting advanced encryption solutions," the note reads. Of course, companies such as Google, Yahoo and Microsoft have already made SSL the default option for their services, in an effort to protect everyone's privacy and some even upgraded the certificates to 2,048 bit, making things even more difficult for anyone trying to snoop in. If the Department has its way, anyone receiving a notice, be it person or company, will be required to provide "information or assistance" to place information obtained under the warrant into an intelligible form. That translates into providing the SSL keys to decrypt data. Failure to comply would constitute a criminal offence, putting everyone between a rock and a hard place. What the Australian authorities are trying to do is to make encryption obsolete. Basically, they don't want anyone to protect their communications in any way and if they dare do so, they should immediately unveil their private conversations when asked. Ever since the NSA scandal broke through, involving numerous countries, including Australia, one of the members of the Five Eyes nations, it seems that governments have stopped hiding behind niceties and started trying to legalize their spying practices. One example is this Australian effort to neutralize encryption, another is the American revived CISPA that would put everyone's privacy at risk. Before this, agencies were secretly sending

requests to providers of web services to obtain the decrypted communications or even asking them to provide master encryption keys, such as the one demand sent to Ladar Levison and his mailing project Lavabit. To read more click **HERE**

Sally Beauty Says Hackers Stole Around 25,000 Payment Card Records

SoftPedia, 18 Mar 2014: Earlier this month, we learned that professional beauty products retailer Sally Beauty suffered a data breach. Initially, the company didn't find any evidence that customer information had been stolen. However, in a statement published on its website on Monday, the company revealed that close to 25,000 customer payment cards had been compromised. It appears that the attackers have managed to steal Track 2 card data, including names, card numbers, expiration dates and CVVs. There's no indication that social security numbers, dates of birth and other sensitive information has been obtained by the cybercriminals. The company doesn't collect any PIN data. "As experience has shown in prior data security incidents at other companies, it is difficult to ascertain with certainty the scope of a data security breach/incident prior to the completion of a comprehensive forensic investigation. As a result, we will not speculate as to the scope or nature of the data security incident," the company stated. The US Secret Service has been called in to investigate the incident. In the meantime, the retailer is taking steps to ensure that its payment card information systems are secured and that servers are malware-free. All security systems are being reviewed. "We take this criminal activity very seriously. We continue to work diligently with Verizon on this investigation and are taking necessary actions and precautions to mitigate and remediate the issues caused by this security incident," Sally Beauty wrote on its website. So far, there's no mention of free credit protection services being offered to affected customers. However, Sally Beauty has promised to provide additional details on how it plans on assisting impacted individuals in the upcoming days. Meanwhile, the company advises customers to check their statements for any suspicious or fraudulent activities, and report any incidents to their financial institution. Customers are also advised to be on the lookout for phishing scams that might leverage the data breach in an effort to trick them into handing over their personal and financial details. Sally Beauty will not ask anyone for sensitive information via email. On Monday, someone breached and defaced Rescator, one of the underground websites responsible for selling payment card data stolen by hackers from Sally Beauty, Target and other companies whose servers have been breached. "To all the people who used this service to blackmail and threaten and 'dox' people's families: [expletive] you especially. To the 'regular' fraudsters: [expletive] you too but slightly less," the hacker wrote on the defaced website. To read more click **HERE**

Car Maker Citroen Hacked, Customer Information Stolen

SoftPedia, 18 Mar 2014: The German website of Citroen, the French car manufacturer, has been hacked by cybercriminals. The company has alerted authorities and an investigation has been launched. According to The Guardian, the attackers planted a backdoor on the shop.citroen.de website, allowing them to steal any data hosted on the webserver. The car maker has determined that some customer information has been compromised, but it's uncertain how many individuals are impacted. Alex Holden of Hold Security has investigated the breach. The backdoor has been removed, but it appears to have been present since August 2013 on the gift site. It's uncertain what type of data has been compromised, but the steps taken by Citroen and the company that operates the website, anyMotion, provide some clues. User and administrator passwords have been reset, purchases have been temporarily disabled, and customers are advised to keep a close eye on their bank accounts. This indicates that some financial information might have been obtained by the hackers. Shipping addresses are also said to have been stored on the compromised server. So how did the cybercriminals breach the Citroen's website? This is where things get interesting. Holden believes these are the same cybercriminals who breached Adobe, PR Newswire and data brokerage companies last year. In most of the attacks, the hackers exploited vulnerabilities in Adobe ColdFusion to gain access to the targeted organization's servers. Brian Krebs, who has been closely monitoring these attacks, has published a new report to reveal that a number of other companies have also been hacked. Elightbulbs.com, a Minnesota-based company that provides lighting solutions, found out that its systems were penetrated back in early November 2013. The company paid a security firm thousands of dollars per year to test the website for vulnerabilities, but the ColdFusion flaws were overlooked for two years.

Following the incident, Elightbulbs.com started outsourcing credit card processing to make sure no customer financial information is stored on their servers. Another lighting company that decided to outsource credit card processing after being hacked by this cybercriminal group was Kichlerlightinglights.com. LaCie, a hardware company owned by Seagate, also learned this week that a server hosting its website has been breached. The company's representatives have told Krebs that so far there's no evidence to suggest that any company or customer data has been compromised. The server hosting LaCie.com was also breached sometime in 2013. Other victims of the cybercrime ring that relies on Adobe ColdFusion exploits are Smucker's and credit card processor SecurePay. To read more click **HERE**

Hacktivists Leak Data from Personal PC of Russian Industrial Investment Fund President

SoftPedia, 18 Mar 2014: Hacktivists of the Russian Cyber Command (Rucyborg) group have announced another data leak. This time, they've targeted the Russian Industrial Investment Fund, a semi-governmental investment company established by a decree of the president of Russia. "Today we aren't going to say much, since we aint got nothing to say pretty much, except that Putin has lost his mind. Russian Industrial Investment Fund is one of the biggest Russian 'non-profit' as they declare organization but they attract investments into Russian economy," the hackers wrote on Cyber Guerilla next to links to the leaked data. They claim to have stolen information from the personal computer of the organization's president, Alexandr Bagnuk. They say the leaked documents contain information on "critical Russian business operations and shadow banking." A total of over 900 Mb of information (750 Mb compressed split up into two files) has been leaked. The hackers have also published a preview consisting of 39 images on imgur.com. A total of 1,400 documents, spreadsheets, image files, archives, PowerPoint presentations and videos have apparently been stolen. Most of the documents are written in Russian, but there are some in English. The files published by Rucyborg also include a copy of Bagnuk's ID card. A lot of other Russian organizations are on the hacktivist group's list of targets. It remains to be seen which one of them is next. There are a lot of cyber operations surrounding Russia these days and Rucyborg's attacks are only a small part of the whole picture. Last week, Rucyborg leaked files from the systems of SearchInform, a Russian company with apparent ties to the FSB. The same group has also stolen data from Rosoboronexport, a major defense-related imports and exports company. Russia has also been targeted by hackers shortly after authorities decided to block several news websites at ISP level. The blocked websites are known for criticizing Russian President Vladimir Putin, but officially, this doesn't have anything to do with the decision. In response to the blockade, a number of government websites, including the one of the Kremlin, were disrupted with DDOS attacks. While no hacktivist groups appear to show support for Russia, at least not directly, one of the country's intelligence agencies is suspected of developing a piece of malware that has been used in numerous cyber espionage operations. This year, the campaign, which has been dubbed "Snake," has mainly targeted Ukraine. The infections coincide with Russia's invasion of Crimea, so the cyberattacks might have been part of an intelligence gathering operation by the Russian government. To read more click **HERE**

Account-hijacking Trojan spreads via Facebook messages

Heise Security, 12 Mar 2014: Private messages delivering what seems to be an image are spreading like wildfire on Facebook, as the file in question triggers the download of a Trojan that compromises the victims' computer and Facebook account to spread the malware further. The infection chain starts like this: the victim sees the message from a friend that simply states "LOL" and includes an image. Unfortunately, the ZIP file in question contains a Java JAR file of the same name that, when run, downloads the actual malware from a remote Dropbox account. The two aforementioned files are not malicious per se, but the third one is - it's a Trojan that injects itself into legitimate processes currently running on the victims' system. According to Malwarebytes' Adam Kujawa, it's still unkown what the Trojan does except compromise the victims' Facebook account, but if we go by the results on VirusTotal, it could be a variant of the infamous Zusy banking Trojan. "The origin of the threat is also currently under investigation however some of the text found within the Java file leads us to believe it was developed by someone who speaks Greek," noted Kujawa. Users are advised not to open automatically similar files received from Facebook friends, but to ask them first if

they were the ones who sent it. "If they don't respond or they say 'I dunno, I didn't send that' then go ahead and suggest your friend run an AV scan and change their Facebook passwords, in that order," he advises. The malware affects only computers running Windows, so if you accessed your Facebook account and tried to open the file via your mobile phone or Mac, you're in the clear. To read more click **HERE**

Rbrute Trojan hacks Wi-Fi routers to help spread Sality

Heise Security, 13 Mar 2014: Researchers from Russian AV company Dr. Web have recently analyzed a Trojan that hacks Wi-Fi routers in order to facilitate the spreading of the infamous Sality malware family. Sality is one of the oldest malware families out there, and its partly due to its spreading and communication capabilities that it has survived for this long. It is capable of a variety of malicious actions, including terminating AV software and firewalls, stealing information from infected computer and using it to spam other users, download additional malware, and so on. It also has rootkit capabilities, and spreads via removable drives and network shares, and in the latest spotted approach, it works in conjunction with the aforementioned Wi-Fi-hacking Trojan - dubbed Rbrute - to propagate itself. "When launched on a Windows computer, Trojan.Rbrute establishes a connection with the remote server and stands by for instructions. One of them provides the Trojan with a range of IP addresses to scan," the researchers explain. In addition to this, Rbrute can mount a dictionary attack on the router. If successful, it reports back to the remote server, which then "instructs" the router to change the DNS addresses stored in its settings. "As a result, when a user tries to visit a website, they can be redirected to another site that has been crafted by intruders. This scheme is currently being used by cybercriminals to expand the botnet created using the malware Win32.Sector," the researchers note. Win32.Sector is just another name for Sality. Rbrute compromises the router so that other machines using it could be ultimately infected. Currently, the malware redirects targeted users to a spoofed Google Chrome download site, where the file offered for download is actually a Sality variant. Once on the computer, Sality downloads Rbrute, and so the infection cycle continues. What can you do to protect your computer and your router from these dangers? Well, a good AV solution should block both, but just in case, change the default settings of your Wi-Fi router, and select an extra complex and long password that can't be easily cracked by brute forcing. In fact, you should do this by default with every new router you set up. Rbrute Trojan can currently crack passwords on a number of different router models, including: D-Link DSL-2520U, DSL-2600U, TP-Link TD-W8901G, TD-W8901G 3.0, TD-W8901GB, TD-W8951ND, TD-W8961ND, TD-8840T, TD-8840T 2.0, TD-W8961ND, TD-8816, TD-8817 2.0, TD-8817, TD-W8151N, TD-W8101G, ZTE ZXV10 W300, ZXDSL 831CII. To read more click **HERE**