THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

14 July 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

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, and Sandia National 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 this open source data

July 11, IDG News Service – (International) **Source code for tiny 'Tinba' banking malware leaked.** Researchers with CSIS Security Group reported that the source code for the Tinba, also known as Zusy, banking malware was posted openly on underweb forums, potentially allowing a greater number of attackers to utilize the malware. The malware is capable of interfering in online banking sessions to steal user credentials and has an unusually small code base. Source: http://www.computerworld.com/s/article/9249670/Source_code_for_tiny_Tinba_banking_malware_leaked

July 10, Securityweek – (International) **Shylock malware infrastructure targeted by international authorities.** Law enforcement agencies in the U.S., E.U. and Turkey along with several security firms conducted a coordinated operation July 8-9 to seize domains and command and control servers used by the Shylock banking malware. The malware, also known as Caphaw, has infected at least 30,000 computers and been in use since 2011. Source: http://www.securityweek.com/shylock-malware-infrastructure-targeted-international-authorities

July 10, Securityweek – (International) **Hackers attack shipping and logistics firms using malware-laden handheld scanners.** Researchers with TrapX released a report stating that an undisclosed Chinese manufacturer of handheld scanners used by shipping, logistics, and manufacturing planted malware on the devices as part of a campaign dubbed "Zombie Zero." The malware attacks company networks once the scanner is connected to the victim's wireless network and sends data to a command and control server located at the Lanxiang Vocational School in China. Source: http://www.securityweek.com/hackers-attack-shipping-and-logistics-firms-using-malware-laden-handheld-scanners

July 10, Securityweek – (International) **Kaspersky Lab details 'versatile' DDoS trojan for Linux systems.** Researchers with Kaspersky Lab reported identifying a Linux distributed denial of service (DDoS) trojan with several modules to add various capabilities. Components of the trojan were identified a Backdoor.Linux.Ganiw.a and Backdoor.Linux.Mayday.f. Source: http://www.securityweek.com/kaspersky-lab-details-versatile-ddos-trojan-linux-systems

July 10, Softpedia – (International) **Gmail for iOS poses man-in-the-middle attack risk.** Lacoon researchers found the Gmail app for iOS can leave users vulnerable to man-in-the-middle (MitM) attacks due to the app lacking the certificate pinning feature. This could allow attackers to use a rogue certificate to impersonate the Gmail server and route traffic through their systems. Source: http://news.softpedia.com/news/Gmail-for-iOS-Poses-Man-in-the-Middle-Risk-450315.shtml

July 10, SC Magazine – (International) **Kaspersky quickly addresses XSS flaw impacting company website.** Kaspersky Lab closed a cross-site scripting (XSS) vulnerability on one of its Web sites after being notified of the issue by a security researcher, the company reported July 10. There was no indication that the flaw was exploited by attackers. Source: http://www.scmagazine.com/kaspersky-quickly-addresses-xss-flaw-impacting-company-website/article/360353/

Cisco Patches Four-Year-Old Apache Struts 2 Issue

SoftPedia, 14 Jul 2014: A vulnerability in Apache Struts 2 that would allow a potential attacker to execute arbitrary code on an affected system has been patched by Cisco at the end of last week; the security issue was initially reported in July 2010. The problem occurred because of improper sanitization of the input in the XWorks component in Apache Struts 2. A malcrafted Object-Graph Navigation Language (OGNL) expression could be used by an attacker to compromise a vulnerable system. As noted in the original report on the issue, identified as CVE-2010-1870, the OGNL expression evaluation relies on a whitelist that does not restrict modification of server-side context objects and circumvent the available "#" protection mechanism in the ParameterInterceptors directive. The list of Cisco products affected by the security issue comprises Cisco Business Edition 3000 Series, Cisco Identity Services Engine (ISE), Cisco Media Experience Engine (MXE) 3500 Series, and Cisco Unified Contact Center Enterprise (Cisco Unified CCE). The company informs that there are free updates mitigating the problem for all of the above products, except Cisco Business Edition 3000 Series. Customers who use this product are advised to "contact their Cisco representative for available options." Where possible, updating to the latest version of the product is the only solution, as Cisco provides no workarounds for mitigating the risks caused by this vulnerability. To read more click **HERE**

Drug Delivery Microchip Spurs Security Concerns

SoftPedia, 14 Jul 2014: A company called Microchips has made headlines these days with a project designed to deliver a birth control drug through a chip implanted under the skin. This is not the only purpose for the micro device, though, as its potential extends to administrating other drugs, too. Taking into consideration the inefficient protection portable medical devices have proven to have, concerns about the security risks for the wearer of this type of microchip arise. The device is conceived with multiple reservoirs protected within the body, each containing the necessary drug dose a patient needs to be delivered. These can be opened on demand or at specific time intervals. Opening them on demand is the concerning part, because, should someone be able to circumvent the built-in protection, the action poses a significant risk for the wearer of the chip. According to the company, activating the delivery of the drug is done through electrical signals that melt the membrane of a reservoir, releasing the content into the body of the patient. The technology has been developed by the scientists at MIT and they licensed it to Microchips, which specializes in medical technology. The drug release signal is sent wirelessly (radio frequency) from a remote control and, as is the case of many wireless technologies, it presents the risk of being hacked. However, Microchips President and COO, Robert Farra, told Mashable that the technology would be built to include security measures, such as a very limited range of the wireless signal sent by the remote control. Farra says that the distance will be of just a few centimeters, which would require a threat actor to get in very close proximity to the victim. The short range does not permit a hacker to intercept the signal, either. Also, it would be possible to set a password for the remote control, although this would not be very reassuring considering the various ways that can be used to find a countersign. At this stage of development, it may appear that there are no feasible ways for a hacker to tamper with the device and the way it releases the drugs, but as it was the case with numerous technologies, means to circumvent security are found most of the time and these generally appear after the technology opens up to a wider audience. The device has already been subject to clinical human trials, on women suffering from osteoporosis, and the results were successful. Both the device and the drug combination were bio-compatible with the patients. To read more click **HERE**

Keyloggers Installed at Hotel Business Centers, the U.S. Secret Service Warns

SoftPedia, 14 Jul 2014: The U.S. Secret Service has sent out an advisory to businesses in the hospitality industry to warn them that their computer systems for guests are targeted by cybercriminals who install keylogging software to steal personal information. The letter was sent on July 10 and informs that suspects conducting this sort of activity in major hotel centers in the Dallas/Fort Worth areas have been arrested. They would access the public computer systems in the business center of a hotel and download keylogging software from a Gmail address in order to install it. The malicious software would

surreptitiously record all activity on the affected computer, collecting personally identifiable details, log-in credentials for bank accounts or various other web services. "The suspects were able to obtain large amounts of information including other guests' personally identifiable information (PII), log in credentials to bank, retirement and personal webmail accounts, as well as other sensitive data flowing through the business center's computers," reads the advisory. All the keystrokes of the guests using the compromised systems would be sent to the criminals' email addresses. There is no information on the number of guests that have been affected by the nefarious activities of the crooks. According to Brian Krebs, who got hold of the advisory letter, several recommendations are provided for increased security of the public computer systems offered by such businesses. One of the measures is to limit the privileges of the account used by guests so that they are restricted from adding and removing new software on the machine. Although this is not a foolproof solution, it may discourage less technical cybercriminals from engaging in such activities. "The attacks were not sophisticated, requiring little technical skill, and did not involve the exploit of vulnerabilities in browsers, operating systems or software. The malicious actors were able to utilize a low-cost, high impact strategy to access a physical system, stealing sensitive data from hotels and subsequently their guests' information," reads the advisory message. As Krebs points out, having physical access to a machine is the easiest way to compromise it, given the multitude of tools that can be used to boot it into a different operating system which allows modifying the data on the original one. Using a public computer for accessing services that hold private information poses a great risk many users are still not aware of. And although there are solutions for ensuring privacy when working on such machines, not all businesses are capable of implementing them, either because of the logistics available or the lack of technical knowledge. As such, it falls on the shoulders of the user to make sure that their private data remains safe from prying eyes. To read more click **HERE**

GameOver ZeuS Is Making a Comeback

SoftPedia, 14 Jul 2014: Despite the efforts of different law enforcement agencies and several private security companies to disrupt a massive GameOver ZeuS botnet in early June, a new variant of the malware has been uncovered. Security researchers from Malcovery say that the mutation they found is fresh, as they found that one of the domains used for command and control activity had been registered on Thursday, July 10, in China, and it was active. The operators of the new GameOver ZeuS strain deliver the malware through spam purporting to be notifications from financial institutions, fake messages from banks such as M&T and NatWest being among the samples caught by the security researchers. The emails come with an attachment, which, once opened, executes the malware payload and communication with command and control servers (C2) is initiated in order to receive instructions. Malcovery security engineers noticed that the fresh variant relies on a domain-generation algorithm (DGA) that "bears a striking resemblance" to the original GameOver ZeuS. DGA is used to generate a large number of random domain names, and only a small amount of them is contacted by the malware in search of one that responds to the requests and provides the instruction set. After contacting the FBI and Dell Secure Works, two of the parties involved in the takedown of the botnet, dubbed Operation Tovar, in early June, Malcovery experts could confirm that the C2 servers used for that botnet were still under their control. In an official statement, the Department of Justice "reported that all or nearly all of the active computers infected with GameOver Zeus have been liberated from the criminals' control and are now communicating exclusively with the substitute server established pursuant to court order." A difference compared to the original malware is that the newly discovered variant no longer uses the peer-to-peer architecture. Furthermore, "in addition to a new DGA, the malware seems to have traded its Peer to Peer Infrastructure for a new Fast Flux hosted C&C strategy," say the security experts in a blog post. The FBI estimated that the GameOver ZeuS botnet led to losses of more than $100 / €73.5 million. Since the source code for GameOver ZeuS was still in the hands of the cybercriminals, this comeback should not come as a surprise. Towards the end of June, security researchers from Arbor Networks announced that they found evidence of an active malicious campaign that was based on the GameOver Trojan and which evaded the takedown. To read more click **HERE**

Diehard Zeus Banking Malware

SoftPedia, 14 Jul 2014: Zeus Trojan has been identified for the first time in July 2007 and the group behind it was arrested in 2010. They used the malicious code to collect credentials for financial institutions and then empty the accounts of the victims. The damage was quite significant at the time, with millions of dollars stolen from banks in the U.K. and the U.S. filling the pockets of the prime suspects. The entire criminal syndicate behind the Zeus/Zbot malware managed to cash in tens of millions of dollars. Yet, seven years later, the Zeus name still makes the headlines of publications in the security industry. The longevity of this malware family, which will soon reach the status of clan, is given by the fact that it was sold on underground websites to anyone who wanted to set up a cybercriminal operation, as long as they had a few thousand dollars. It was offered as a ready-made kit, with instructions on how to build the Trojan, but the success of the operation depended on how business-savvy the cybercriminals were. Apart from this, its source code leaked in 2011, and initially, it was up for grabs only from specific locations, but now it can be found with a single Google search. Of course, given the time that went by and the advancements in security, it is more suited for study rather than for starting a "business." This stimulated other cybercriminals to analyze the original version of the malware and apply their own optimizations to make it resilient to antivirus detection. After several unfitting variants, the underground forums were provided with a new malware kit derived from Zeus code, called Citadel. The operation worked for at least one year and a half, until Microsoft announced in June 2013 that the command and control servers for the botnets created by Citadel had been seized and were under the supervision of the good guys. Numerous law enforcement entities and multiple security companies in the private sector contributed to disrupting the botnets. The lawsuit that ensued included a total of 82 defendants, all being accused of controlling a computer botnet. The number of botnets and infected computers was so large that Microsoft did not manage to finish the sink-hole process two months after it started. Specifically, Citadel had spawned 1,462 botnets, while the number of infected computers amounted to millions. One would think that this sort of engagement and dedication to disrupt this type of malicious actions would have caused the cyber-crooks to lay low for a while. However, the organized crime regrouped quickly and came up with a new, significantly enhanced variant of Zeus, called GameOver Zeus, which was tightly controlled by a core group in Russia and Ukraine since October 2011. On June 2, 2014, the GameOver Zeus botnet was dismantled in what was called Operation Tovar, but not completely disrupted, because the operators used a decentralized system of proxies and strong encryption to keep the master servers hidden. This strain was not available for sale and, according to the U.S. Justice Department, it was employed in the theft of more than $100 million (€73,5 million). Its operators would hit high-dollar corporate accounts that were preceded by large distributed denial-of-service (DDoS) attacks in order to distract the victim from the account take-over activity. In recent reports from security researchers, the GameOver Zeus malware is making a comeback, a little over a month after dismantling the botnet. This was to be expected given the complex nature of the network and the fast regrouping ability of the cybercriminals. Again, this is not the same code used for creating the previous botnet. The malware developers integrated new features and protection mechanisms to ensure the longevity of the malicious campaign. However, more concerning is the fact that despite all the impressive efforts made to take down the criminal organizations using Zeus-based malicious tools, some of them managed to slip through the cracks. It has been reported recently that a group of cybercriminals successfully evaded the Citadel take-down in 2013 as well as the latest attempt from law enforcement to disrupt the GameOver Zeus operations, in June 2014. The lucky crooks continued to work with Citadel until the end of 2013, when they switched to the GameOver Zeus malware. When Operation Tovar was deployed, this group remained untouched for the second time and kept on with their activity. Apart from this, smaller variants of Zeus continue to appear; some are the work of less ambitious developers, others present evidence of professionals being involved in the creation and optimization of the code. It may not take long until a new malware family replaces Zeus and buries it in the history pages of the security industry, but its resilience against the deployment of forces that include law enforcement agencies and leading security companies around the globe is definitely increasing the standard in malware writing. To read more click **HERE**

Private Health Info on More than 20,000 Children Leaked

SoftPedia, 11 Jul 2014: Information leaks should not always be blamed on hackers taking advantage of weak security systems. This sort of incident sometimes occurs because of the carelessness of employees that manage somehow to place the sensitive details in the wrong inboxes. This is the case with private health info of more than 20,000 children that benefited from treatment at Rady Children's Hospital in San Diego. It seems that all this data was sent, by mistake, to the email addresses of job applicants. U-T San Diego reports that the hospital employees managed to do this mistake not just once, but twice. The first batch of details, which was enclosed in a spreadsheet file, contained information about 14,121 patients, consisting in names, dates of birth, primary diagnoses, admittance and discharge dates, medical record numbers and other details like insurance claim data. This was sent to the email inbox of four job applicants, who, in turn, forwarded the file to another two individuals. As such the details were exposed to a total of six, but two of them could not open the document. While investigating this incident, the hospital representatives said that they found evidence of a similar leak, this time with info on 6,307 patients, registered for treatment between June 30, 2009 and June 30, 2010. The details leaked to third-party individuals contained names, discharge dates, the locations where they were treated, and account info (name of the insurance company, outstanding balance). The spill was larger in this case because, besides sending the info to three candidates, six more were able to access it when they took a test on the company's computers. Sensitive and confidential details should always be protected and stored securely on systems that are not accessible from any computer in the building, and certainly not without authentication. A spokesperson for Rady Hospital, Ben Metcalf, told U-T that the first leak happened because the employee attached the wrong file to the email for the candidates. He explained the second incident by saying that the employee "did not realize that the information constituted protected health information." He also said that in both cases, the intended purpose of the files for the job applicants was to judge their skills as part of the hiring process. In order to prevent such embarrassing cases in the future, Metcalf announced that the hospital reviewed the evaluation process of the candidates and imposed the use of only validated testing programs. Furthermore, the employees are to improve their computer skills and ability to recognize confidential information through new training processes. The parents of the children affected by the incident have been notified of the data leak via email. To read more click **HERE**

Romanian Receives Almost Four Years of Jail Time for Phishing

SoftPedia, 11 Jul 2014: Iulian Schiopu, of Craiova, Romania, was sentenced to serve 45 months in a federal prison for his involvement in a phishing scheme perpetrated against customers of multiple American banks in June 2005. He was part of a group of 19 Romanian nationals that targeted financial institutions and companies, such as Citibank, Capital One, Bank of America, JPMorgan Chase & Co., Comerica Bank, Regions Bank, LaSalle Bank, U.S. Bank, Wells Fargo & Co., eBay and PayPal, through phishing campaigns. The court documents show that a resident of Madison, Connecticut, received a suspicious email with a link that led to a phishing page for People's Bank. A classic lure was used: the message informed that access to the online bank account had been blocked and it would be unlocked as soon as some information was entered. This, of course, consisted of all the details necessary to log into the account and to withdraw the money. "The web page appeared to originate from People's Bank, but, as the investigation revealed, was actually hosted on a compromised computer in Minnesota," says the news release from the FBI. All the information would then be sent to an email account under the control of the cybercriminals, who would use it to cash the money from ATMs, some of them in Romania. The investigation revealed thousands of emails with data collected from the victims: credit or debit card numbers, expiration dates, CVV codes, PIN numbers. Additional personal identification information such as names, addresses, telephone numbers, dates of birth, and Social Security numbers, was also found. Schiopu, aged 34, was arrested in Sweden on May 7 and extradited to the United States on September 12, 2013. Deirdre M. Daly, United States Attorney for the District of Connecticut, acknowledged the critical assistance provided by the U.S. Department of Justice Office of International Affairs, the FBI Legal Attaché in Bucharest, Interpol, the Romanian National Police and the United States Marshals Service.

Phishing schemes are one of the most popular methods for deceiving computer users not just to access a web page that pretends to belong to the victim's bank, but also for distributing malware that can lead to financial fraud. Well-organized cybercriminals launch these campaigns in waves and use multiple forms of incentives. The general recommendation is to refrain from accessing links that have a dodgy origin. Moreover, things that seem too good to be true are most of the times an attempt to trick the user into getting their machine infected. To read more click **HERE**