THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

18 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 17, Help Net Security – (International) **63% of businesses don't encrypt credit cards.** SecurityMetrics found in a study that 63.86 percent of businesses surveyed store unencrypted 16-digit payment cards on their systems, and 7 percent store magnetic stripe data, providing easy targets for fraud, among other findings. Source: http://www.net-security.org/secworld.php?id=17135

July 17, The Register – (International) **Pushdo trojan outbreak: 11 THOUSAND systems infected in just 24 hours.** Bitdefender researchers reported that a new campaign to spread the Pushdo botnet malware compromised over 11,000 systems within a 24-hour period, with the majority of infected users in Asia and some in the U.S., U.K., and France. The Pushdo botnet has previously been used in spam campaigns and to distribute malware such as Zeus and SpyEye. Source: http://www.theregister.co.uk/2014/07/17/pushdo_trojan_outbreak/

July 17, Softpedia – (International) **Cisco patches critical issue in wireless residential gateway products.** Cisco released patches for several Cisco Wireless Residential Gateway products, closing a vulnerability that could allow attackers to use malicious HTTP requests to crash the Web server and inject commands or execute code with elevated privileges. Source: http://news.softpedia.com/news/Cisco-Patches-Critical-Issue-in-Wireless-Residential-Gateway-Products-451109.shtml

July 17, Softpedia – (International) **SQL injection risk in vBulletin receives prompt patch.** vBulletin released a patch for its forum software which closes a SQL injection vulnerability that was identified and disclosed by Romanian Security Team. Source: http://news.softpedia.com/news/SQL-Injection-Risk-in-vBulletin-Receives-Prompt-Patch-451090.shtml

July 17, Softpedia – (International) **Critical vulnerabilities fixed in Drupal 7.29 and 6.32.** The Drupal Security Team advised all users to update to versions to 7.29 or 6.32 in order to close vulnerabilities that could allow attackers to perform denial of service (DoS) attacks cross-site scripting (XSS) attacks. Source: http://news.softpedia.com/news/Critical-Vulnerabilities-Fixed-in-Drupal-7-29-and-6-32-451074.shtml

July 17, Threatpost – (International) **Five vulnerabilities fixed in Apache Web Server.** The Apache Software Foundation released version 2.4.10-dev of its Apache Web Server, closing five vulnerabilities, including a buffer overflow vulnerability and several denial of service (DoS) vulnerabilities. Source: http://threatpost.com/five-vulnerabilities-fixed-in-apache-web-server/107278

72% of Fraud Victims in Chicago Resulted from Data Breaches
SoftPedia, 18 Jul 2014: According to a new study, most of the Chicago citizens who have been victims of various types of online fraud have also been victimized by cybercriminals' unauthorized access to their personal information. The research was released by the National Consumers League (NCL) and Javelin Strategy. The connection between data breaches and fraud is easy to make, as threat actors seek to copy private details of individuals from various systems to specifically use them in fraudulent activities. At an event about the security of information, Attorney General Lisa Madigan said that "the latest data breaches have served as a wakeup call signaling that government and the private sector need to take serious,

meaningful action to curb this growing threat to our financial security." According to NCL, the consumers expressed their desire for the government to take more action regarding fraud prevention, as they are losing confidence in the protection abilities of businesses handling sensitive information. John Breyault from NCL said that consumers expect their information that is shared with both private and government entities to be kept safely and protected from threat actors. According to the study, about half (49%) of all the fraud victims are not aware of the entity responsible for the compromise of their personal details. However, the state of Illinois has enacted legislation (Personal Information Protection Act) that requires private and government entities to notify individuals of security breaches that involve personally identifiable information; this includes the name combined with the Social Security number, driver's license number, as well as financial details. The research was carried out on residents in Chicago, Los Angeles, Miami and Minneapolis. It states that 72% of the fraud victims in Chicago had been previously served a breach notification letter. Comparatively, 66% of fraud victims in Minneapolis received an alert, and the highest number of such cases was recorded in Los Angeles (82%) and Miami (80%). NCL says that last year more than 550 million identities were compromised in 614 data breach incidents, which led to fraudulent activity costing hundreds of millions of dollars. They give as example the attack on Target, which cost credit unions and community banks about $200 / €148 million for re-issuing 21.8 million credit and debit cards. The results of the fresh research lead to multiple consequences, such as the fact that consumers are losing their trust in businesses on whose systems their data was compromised. This, in turn, leads to decreased sales for retailers, thus posing economic problems. To read more click **HERE**

Romanian Cybercriminal Ring Dismantled by European Law Enforcement

SoftPedia, 18 Jul 2014: An organized crime network composed of more than 100 individuals, most of them Romanian nationals, has been dismantled by the European Cybercrime Centre (EC3) at Europol and law enforcement agencies in France and Romania. The cybercriminals conducted payment crimes that involved intrusions into international non-cash payment systems, through malware infections of computers. They would compromise the machines of franchisees authorized to perform money transfers using a remote access tool that integrated key-logging functionality. According to information from the Directorate for Investigating Organized Crime and Terrorism (DIICOT), the gang targeted the computer systems of copy-shop businesses located in Austria, Belgium, Germany, Norway, and the UK, that would also have installed money transfer services. After stealing the operator's credentials, they were able to initiate money transfer orders from a fictitious sender to a real individual who was usually based in Romania and who would pick up the money from another operator. This activity would sometimes be carried out using mobile phones. DIICOT says that the money losses were entirely supported by the affected franchisees, and as a result of this sort of fraudulent activity, one of them registered a loss of more than $800,000 / €591,000. Europol estimates that the total prejudice created by the cybercriminal organization is of at least €2 / $2.7 million. "The proceeds of their crimes were invested in different types of property, deposited in bank accounts or transferred electronically to hide their illicit origin." Out of the more than 115 individuals suspected of having ties with the criminal group, 65 were detained as a result of coordinated raids that took place at addresses in Romania and France. The authorities seized large amounts of money, luxury cars, and IT equipment. About 450 police officers were involved in the operation and 117 house search warrants were executed, 112 at addresses in Romania. Europol and DIICOT found evidence that this was not the only illicit activity conducted by the crime group, as they were also involved in card skimming in the metropolitan area of Paris and drug trafficking. "As a direct result of the excellent cooperation and outstanding work by police officers and prosecutors from Romania, France and other European countries, a key criminal network has been successfully taken down this week. EC3's role was to effectively facilitate international cooperation, including the exchange of intelligence, and to provide resources where needed. "After many months and a great effort from all involved, many individuals have now been detained after key locations were identified and targeted by law enforcement," said Troels Oerting, Head of the EC3. The law enforcement agencies involved in dismantling this crime ring included DIICOT from Craiova city, Romanian National Police and the Brigade for Combating Organized Crime from Craiova, the Service of Intelligence and Internal Protection (DGIPI) from the same

city, the National Intelligence Service (SRI), and the Brigade of Combating Payment Fraud in Paris of the Judicial French Police (BFMP DPJ). To read more click **HERE**

Phishing Duo in the UK Sentenced to 14 Years in Jail

SoftPedia, 18 Jul 2014: Two individuals, a male and a female, have been sentenced to eight and six years of prison time, respectively, as a result of running phishing scams from the United Kingdom on unsuspecting users. According to London Metropolitan Police, the duo, identified as 23-year-old Constanta Agrigoroaie and 28-year-old Radu Savoae, pleaded guilty on Thursday to conspiracy to commit fraud, six counts of possession of fraudulent ID cards, and possessing equipment to make fraudulent ID and bank cards. They are Romanian nationals and reside in Mornington Avenue, Ilford, from where they sent phishing emails to more than 150 victims. The luring message purported to be from Apple and informed that the victim's account had been compromised, urging them to update their details through a link to the phishing website. The requested information also includes bank details, and once entered in the respective fields, the cybercrooks would receive it via email. They would then use it to extract large amounts of money. The police say that the perps managed to steal more than £15,000 / €19,000 / $25,600 from victims in the United Kingdom, which would be used for buying travel tickets for Romanian pickpockets who operated on London's transport network. The fraudulent activity of Agrigoroaie and Savoae was discovered as a result of a joint operation by detectives from the Metropolitan Police Service and Bedfordshire Police at Luton Airport, when a flight from Romania was intercepted. Six passengers claiming they did not know each other had tickets bought through the same computer. Further investigation led to the phishing duo's address. "Investigation into these bookings revealed an address in Ilford was responsible for the purchase of the tickets and on 4 April, officers searched the address where they found Agrigoroaie sitting in front of a computer looking at websites belonging to east European airlines," reads the news from the Metropolitan Police. It appears that she also had a script open, with numerous personal details of the scammed victims; this included bank card information with the full 16 digit number, expiry date and CVV number, as well as home addresses. During the raid, police officers found multiple laptops, iPads, printers and the necessary tools for cloning credit cards. The two scammers conducted fraudulent activities on computer users from around the world. "This 'phishing' duo took advantage of many internet users and duped them into providing their personal information. However as a result of a tireless investigation by the RTPC, they have been jailed which has no doubt prevented numerous bank customers from becoming victims of this crime," said Chief Superintendent Matt Bell, Roads and Transport Policing Command. To read more click **HERE**

Info on 1,700 Individuals Accessed from Energy Company Subcontractor's Systems

SoftPedia, 18 Jul 2014: Personal information of Dominion Resources' employee's wellness plan has been accessed without authorization by an unknown intruder through the systems of a subcontractor. The data, which includes names, addresses, email addresses, phone numbers, gender and dates of birth, has been reached through the computer systems of Onsite Health Diagnostics. The breach took place on March 25 but it was not detected immediately, and Onsite Health Diagnostics alerted StayWell Health Management, the vendor of employee wellness programs, on June 16. A week later, on June 24, Dominion Resources was notified that the details of 1,700 of their employees had been accessed during the intrusion. At that moment, the identities of the individuals impacted by the attack were not known, and they were revealed only on July 7, according to Times Dispatch. It appears that the information accessed by the intruder belonged to individuals that had made health-screening appointments as far back as 2012. They were alerted to change their passwords and were offered one year of free credit monitoring in order to protect their accounts from fraudulent activities. The detection of the intrusion and alerting Dominion Resources both took very long, and the affected company is currently checking why the notification action was delayed so much. A representative also said that Onsite Health Diagnostics was no longer used by them for making health-screening appointments. Dominion Resources is a power and energy company headquartered in Richmond, Virginia. There is no evidence that the details accessed by the intruder have been misused. To read more click **HERE**

Engineer Arrested Over Massive Benesse Holdings Data Leak

SoftPedia, 18 Jul 2014: The Tokyo Metropolitan Police Department announced on Thursday, July 17, the arrest of a systems engineer for allegedly stealing private information of about 7.6 million customers of the education service provider Benesse Holdings. Last week, the company announced that the incident, which is considered one of the largest ever in Japan, could actually involve details of 20.7 million customers. The discovery was made when affected customers reported receiving direct email messages and phone calls from businesses in the education sector pitching them sales offers, although they had not disclosed personal information to them. The companies were not connected with Benesse Holdings, which is the parent of Berlitz language schools in Japan. At the beginning of the investigation, the Metropolitan Police Department believed that an outsider was responsible for the incident; however Benesse's checks of the systems did not reveal traces of a breach. According to local media, 39-year-old Masaomi Matsuzaki was employed at the Tokyo branch in Tama of Synform Co., which is a company within the Benesse Holdings group. He is accused of illegal access to the company's systems and stealing the customer data with the purpose of selling it. According to Japanese media, it appears that the system engineer gone rogue managed to trade the info for several millions of yen, which would amount to tens of thousands of dollars/euros. The reason of the intrusion seems to be the fact that he had debts of hundreds of thousands of yen accumulated on gambling and living expenses. Using his credentials, Matsuzaki copied the information from the systems of the company on a removable storage device and sold it to a dealer for the unspecified amount. Local media reports that he admitted to this during questioning. The stolen data referred to customers that had purchased educational products (courses and magazines) and included names, birth dates, home addresses and phone numbers. Financial details (credit card numbers, bank accounts) could also have been leaked, although there is no confirmation of this. According to the company, Deputy Chairman Tamotsu Fukushima, who was CEO of Benesse Holdings at the time of the leak, and one of the directors, Eiji Aketa, who was president of Benesse Corp. at the time, will step down from their positions after the investigation finishes. In an official notice and apology letter released on July 9, the company said that all affected parties would be notified as soon as they are identified as a result of the internal investigation and the police verfications. To read more click **HERE**

Root Escalation Flaw and Other Issues Fixed in Ubuntu 14.04 LTS with New Kernel Upgrade

SoftPedia, 18 Jul 2014: Quite a few Linux kernel vulnerabilities discovered in the Linux kernel affecting the Ubuntu 14.04 LTS (Trusty Tahr) operating system have been fixed by the developers. The Linux kernel currently used in Ubuntu 14.04 LTS reached end of life soon after the launch of the operating system, but Canonical picked up its maintenance and the devs are now working to implement fixes and other changes. "Sasha Levin reported a flaw in the Linux kernel's point-to-point protocol (PPP) when used with the Layer Two Tunneling Protocol (L2TP). A local user could exploit this flaw to gain administrative privileges." "Salva Peiró discovered an information leak in the Linux kernel's media-device driver. A local attacker could exploit this flaw to obtain sensitive information from kernel memory," reads the official security notification. These are just two of the vulnerabilities closed by this update, which should arrive on the regular channels when using the Software Updater. The security flaws can be fixed if users upgrade the system(s) to the linux-image-3.13.0-32-generic, (3.13.0-32.57), but this is only true for Ubuntu 14.04 LTS (Trusty Tahr). Other operating systems feature different Linux kernels and the versions will be different. ATTENTION: Due to an unavoidable ABI change, the kernel packages have a new version number, which will force you to reinstall and recompile all third-party kernel modules you might have installed. Moreover, if you use the linux-restricted-modules package, you have to update it as well to get modules that work with the new Linux kernel version. To read more click **HERE**

Neverquest Banking Trojan Expands List of Targets

SoftPedia, 18 Jul 2014: Recent variants of the malware analyzed by security researchers show that the cybercriminals operating the Neverquest banking Trojan have focused their attack on banks in the United States and Japan. New telemetry results from Symantec inform that the largest number of infections since December 2013, have occurred in these two countries, accounting for more than half of the

compromised computers. The U.S. recorded 38.51% of the detections, while in Japan the infection accounted for 18.21%. Next in line are Germany (11.48%) and United Kingdom (11.19%). Identified by Symantec as Snifula, in 2014 the malware recorded a spike in Japan for the month of March. Neverquest has been around for a long time, since 2006, and the cybercriminals kept improving its malicious components. At the moment, it is capable to log keystrokes, grab screen captures and record video, control the infected machine through remote control software, as well as steal information using man-in-the-browser (MitB) technique. Symantec also warns that it can steal digital certificates. Exfiltrating the information is done to command and control servers operated by the threat actors. It appears that the remote machines are also contacted for receiving configuration files customized for each target. Security researchers found different configurations for banks located in the U.S., Germany and Japan. They analyzed this data and concluded that it can be separated into two parts, one with code for MitB attack and the other containing a set of strings that trigger monitoring when the victim navigates to a website whose URL includes a match for one of the strings. This is most likely to collect new information about potential targets and prepare attack techniques for compromising them. According to Symantec's research, "There are no major differences between configurations for the US and Japan in terms of the list of strings. We can see around 400 strings related to social networking, customer relationship management, Web mail, messaging, cloud computing, storage, financial, online movie, photo sharing, and gaming services. It seems that most major online services, for both consumer and enterprise users, are covered." The company also says that eight Japanese banks are targeted by the latest version of Neverquest, and ten German ones; however, the figures do not compare with the more than 50 found in the configuration file for the U.S. It appears that Japan has popped on the radar of cybercriminals lately, as ESET details about a banking malware, identified as Win32/Aibatook, that has been distributed through compromised Japanese adult websites. To read more click **HERE**

New Android Ransomware Locks Device Completely

SoftPedia, 18 Jul 2014: Android users are a constant target for cybercrooks, who have released a new scareware with ransomware capabilities that locks the mobile phone completely. The fresh piece poses as a legitimate app that can be downloaded from third-party Android software repositories, and asks for administrator privileges. Once the elevated permissions are obtained, it automatically blocks the phone with a ransom message purporting to be from the FBI. Access to data or any function of the device is restricted, making it inoperable. Researchers at Lookout security firm say that navigating to a different app is not possible because the malicious app, which they named ScarePakage, uses a Java TimerTask to kill any processes unrelated to the malware every ten milliseconds. Moreover, the cybercriminals integrated a wave lock mechanism designed to instruct Android that the app needs to stay on, which prevents the phone from entering sleep mode. The ransom message displayed on the screen purports to be from the FBI and informs that the lock has been enabled due to violation of federal laws of the United States that prohibit visiting online locations that provide pornographic content involving children, animals, as well as child abuse and spamming. Lookout says that several hundred dollars are requested via a MoneyPak voucher in order to unlock the device. However, they also report that the app does not actually check if the voucher code works and only validates its correct length. This could mean that the victim can provide a random code to unlock the phone, provided that they have the correct length of a MoneyPak voucher. However, this has not been confirmed by Lookout, as they did not immediately reply to our request. [UPDATE, July 18] Following our inquiry, a response from Lookout came in, from Jeremy Linden, Senior Security Product Manager: "Some variants of ScarePakage will uninstall themselves if you enter a random, long-enough number to satisfy the MoneyPak demand. However, this is not the case with all variants and there's always the risk that the malware authors will create future functionality to harm the user if they input incorrect data. Using preventative measures is always a better choice." According to the security researchers, the malicious app masquerades as an Adobe Flash package, and in some cases, as an antivirus solution which even starts a scan of the device. Of course, the verification is fake, and as soon as it completes, the lock is applied to the phone. Restarting the device does not disable the ransomware because "a boot receiver class resumes ScarePakage's takeover of your device immediately, shutting

down all other processes that the user interacts with," says Meghan Kelly on the Lookout blog. One precaution that could prevent having the device infected with this malicious app implies avoiding to download packages from sources outside Google Play Store. Also, another way is to not give administrator privileges to apps that have not been verified as being delivered by trusted developers. ScarePakage does not need the phone to be rooted in order to render it inoperable; it only needs elevated privileges. To read more click **HERE**

Botnets gain 18 infected systems per second

Heise Security, 17 Jul 2014: "According to industry estimates, botnets have caused over $9 billion in losses to US victims and over $110 billion in losses globally. Approximately 500 million computers are infected globally each year, translating into 18 victims per second," Joseph Demarest, assistant director for FBI's Cyber Division, has shared on Tuesday with the US Senate subcommittee on crime and terrorism. The affect financial institutions, businesses, universities, hospitals, defense contractors, government, and private citizens, he said, and can be used for DDoS attacks, proxy and spam services, malware distribution, covert intelligence collection, attacks against Internet-connected critical infrastructure, and as weapons in ideology campaigns. Pointing out the facility with which botnet operators infect users' computers and rope them into their malicious networks, he nevertheless proudly noted that the bureau, along with its law enforcement and private sector partners, has been successful in taking down a number of large botnets. "The FBI has developed a strategy to systematically identify cyber criminal enterprises and individuals involved in the development, distribution, facilitation, and support of complex criminal schemes impacting US systems. This complete strategy involves a holistic look at the entire cyber underground ecosystem and all facilitators of a computer intrusion," he shared. "Just last month, the FBI Cyber Division evolved to create a threat-model approach to address the most significant domestic and international cyber threats. He noted the importance of collaboration between the bureau and its international allies, as well as with the private industry and academia, and he mentioned past successes, as well as the latest one: the recent disruption of the GameOver Zeus botnet. To read more click **HERE**

Government-Grade Stealth Malware in Hands of Criminals

Dark Reading, 17 Jul 2014: "Gyges" can be bolted onto other malware to hide it from anti-virus, intrusion detection systems, and other security tools. Malware originally developed for government espionage is now in use by criminals, who are bolting it onto their rootkits and ransomware. The malware, dubbed Gyges, was first discovered in March by Sentinel Labs, which just released an intelligence report outlining their findings. From the report: "Gyges is an early example of how advanced techniques and code developed by governments for espionage are effectively being repurposed, modularized and coupled with other malware to commit cybercrime." Sentinel was able to detect Gyges with on-device heuristic sensors, but many intrusion prevention systems would miss it. The report states that Gyges' evasion techniques are "significantly more sophisticated" than the payloads attached. It includes anti-detection, anti-tampering, anti-debugging, and anti-reverse-engineering capabilities. Because of this, the researchers suspected that although Gyges was attached to ransomware (including CryptoLocker) and bot code, it had been originally created as a "carrier" for a much more sophisticated attack -- something like what a government agency would use to collect intelligence data. Further analysis bears out that suspicion. Certain components of the code matched that of known malware, which had been used before in targeted attacks for an espionage campaign originating in Russia. "This code is really hard to replicate," says Udi Shamir, Sentinel's head of research, "so it would be hard to believe that it was created by a different group." Gyges goes to great lengths to hide itself. For example:

- Lots of malware leaps into action when a user is active; thus, sandbox-based security tools often emulate user activity to trigger malware execution. Gyges, on the other hand, waits for user inactivity before operating.

- It also uses a hooking bypass technique that exploits a log bug in Windows 7 and 8. Security tools could hook into Windows-on-Windows to see what 32-bit applications are trying to run on a 64-bit system. What Gyges can do is start as a 32-bit application, then call the 64-bit system directly, instead of working through Windows-on-Windows, thereby bypassing a hook.

- Gyges also uses Yoda, a "protector," which obfuscates malicious behavior by first converting the original application into sections, then extracting those sections only when the application is running.

"Malware hackers know that at some point they're going to be detected," says Sentinel Labs CEO Tomer Weingarten. "So [the Gyges writers] also started focusing on what happens after they're detected. They're putting in mechanisms to make it very hard for vendors to analyze them." The malware was used by government agencies to gather information -- eavesdropping, keylogging, capturing screens, and stealing identities and intellectual property. Now it is being used by cybercriminals for committing online banking fraud, encrypting hard drives to collect ransoms, installing rootkits and Trojans, creating botnets, and targeting critical infrastructures. Gyges seems like an awfully sophisticated bit of kit to tack onto some run-of-the-mill malware. Why put lipstick on a pig? According to Weingarten, evasion techniques like these can give financially motivated criminals more bang for their buck, better return on their investments, because it helps increase the rate of and duration of infection. "This is definitely a trend we're seeing," he said. "The evasion code is becoming what malware is all about." To read more click HERE

Feds: We beat down Cryptolocker malware, but creator remains at large

Tech Times, 15 Jul 2014: The Department of Justice reports that the Cryptolocker ransomware virus is no longer a threat. By seizing control of the command and control servers for the program, the DoJ has removed Cryptolocker's ability to operate. Cryptolocker needs to communicate with the servers to encrypt the files on an infected computer. The owner would then be asked to pay to regain access to the files. The DoJ is now redirecting the traffic that would go to the Cryptolocker servers, making it impossible for the virus to encrypt any files even if it infects a computer. The department also neutralized Gameover Zeus, a network of infected computers that were used to gain access to financial information and steal millions of dollars. "We succeeded in disabling Gameover Zeus and Cryptolocker only because we blended innovative legal and technical tactics with traditional law enforcement tools and developed strong working relationships with private industry experts and law enforcement counterparts in more than 10 countries around the world," says Deputy Attorney General James Cole in a statement. The DoJ filed a status update with a federal court saying that all or nearly all of the computers infected with Cryptolocker were being successfully redirected to DoJ servers when attempting to communicate with command and control. Traffic directed at the Gameover Zeus botnet is also being redirected. Although more than 137,000 computers remain infected, the communications intercept prevents commands from reaching those computers. The DoJ has set up a website to assist those whose computers are infected with removing the malware. Although the threat has been neutralized, the group of cyber criminals responsible for it has not. Evgeniy Bogachev is suspected of being the leader of the group, which operated out of Russia and Ukraine. He remains at large, and is currently featured on the FBI's Cyber Most Wanted List. Bogachev's group is rumored to have already begun developing and distributing a new malware program to replace Gameover Zeus. The DoJ is confident that the threat of the existing malware programs has been permanently eliminated, but will be issuing an update Aug. 15 to re-examine the situation. To read more click HERE

Why password managers are not as secure as you think

ComputerWorld, 16 Jul 2014: University researchers have raised concerns about the security of web-based password managers that free people from the burden of having to remember website credentials. Scientists at the University of California, Berkeley, studied five password managers and found

vulnerabilities in diverse features like one-time passwords, shared passwords and "bookmarklets," which are used to sign into websites on mobile browsers. "The root causes of the vulnerabilities are also diverse: ranging from logic and authorization mistakes to misunderstandings about the web security model," the researchers said in a paper scheduled to be presented in August at the Usenix Security Symposium in San Diego. "Our study suggests that it remains to be a challenge for the password managers to be secure," the researchers said. The five password managers studied were LastPass, RoboForm, My1login, PasswordBox and NeedMyPassword, all of which run in a Web browser and represent millions of users. Password managers are popular because they require the user to remember only one master password. While all the managers had flaws, the researchers said four of them had vulnerabilities an attacker could exploit to steal users' credentials for arbitrary websites. Overall, the researchers found such a variety of vulnerabilities that they believed password managers were dropping the ball on security. "Password managers handle exceptionally sensitive data — the keys to the kingdom, so to speak," Devdatta Akhawe, co-author of the research, told CSOonline. "As a result, we believe, it behooves them to adopt a higher-than-usual defensive posture while writing these applications and adopt classic principles like least-privilege, defense-in-depth, and open protocols or designs." The researchers reported their findings to the vendors in August 2013. Four responded in a week and have fixed all the major vulnerabilities. Only one, NeedMyPassword, has not responded. In a blog post, LastPass acknowledged fixing the bookmarklet flaw, and said the feature was used by less than 1 percent of its user base. People who used the feature before September 2013 on non-trustworthy sites may consider changing their master password and generating new passwords, but "we don't think it is necessary," the vendor said. Another vulnerability found in LastPass and some of the other vendors let an attacker create a bogus one-time-password to a user account, if the person visited an attacking site while logged into the password manager. However, the attacker would have to know the person's username and still would not have the key to decrypt user data, LastPass said. That flaw was also fixed. The researchers found that some of the password managers were also vulnerable to cross-site request forgery and cross-site scripting attacks. Other flaws made it possible to share a user's credentials with a bogus account, while others made users of some of the password managers vulnerable to phishing attacks. To read more click **HERE**

65 challenges that cloud computing poses to forensics investigators

Heise Security, 16 Jul 2014: The National Institute of Standards and Technology (NIST) has issued for public review and comment a draft report summarizing 65 challenges that cloud computing poses to forensics investigators who uncover, gather, examine and interpret digital evidence to help solve crimes. The report, NIST Cloud Computing Forensic Science Challenges (**link**), was prepared by the NIST Cloud Computing Forensic Science Working Group, an international body of cloud and digital forensic experts from industry, government and academia. Through the report, the working group aims to initiate a dialogue on forensic science concerns in cloud computing ecosystems. "The long-term goal of this effort," explains NIST's Martin Herman, co-chair of the working group, "is to build a deeper understanding of, and consensus on, the high-priority challenges so that the public and private sectors can collaborate on effective responses." The ultimate in distributed computing, cloud computing is revolutionizing how digital data is stored, processed and transmitted. It enables convenient, on-demand network access to a shared pool of configurable computing resources, including servers, storage and applications. Benefits include cost savings, convenience and greater flexibility in how businesses and other consumers employ information technology. The characteristics that make this new technology so attractive also create challenges for forensic investigators who must track down evidence in the ever-changing, elastic, on-demand, self-provisioning cloud computing environments. Even if they seize a tablet or laptop computer at a crime scene, digital crime fighters could come up empty handed if these devices are linked to pooled resources in the cloud. Technical challenges—the focus of the draft report—abound, but almost all intersect with legal and organizational issues. The 65 challenges that the working group identified are divided among nine categories. These include architecture, data collection, analysis, standards, training and "anti-forensics" such as data hiding and malware. To read more click **HERE**