THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

21 October 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

October 20, The Register – (International) **Microsoft pulls another dodgy patch.** Microsoft stated that it is investigating a patch for Windows 7 and Windows Server 2008 R2 after some users reported experiencing issues with their systems after installation. Microsoft advised users experiencing problems to uninstall the patch. Source: http://www.theregister.co.uk/2014/10/20/microsoft_pulls_ianotheri_dodgy_patch/

October 18, Softpedia – (International) **Dropbox users are served a phishing page delivered over SSL.** A researcher with Symantec stated that attackers are using a phishing campaign with a page hosted on Dropbox to attempt to steal users' Dropbox and email credentials. The phishing page uses the secure sockets layer (SSL) protocol of its host in order to appear legitimate. Source: http://news.softpedia.com/news/Dropbox-Users-Are-Served-A-Phishing-Page-Delilvered-Over-SSL-462514.shtml

October 17, The Register – (International) **Apple releases MEGA security patch round for OS X, Server and iTunes.** Apple released a round of patches for several of its products, including OS X, OS X Server, and iTunes, addressing 150 issues including patches to close the POODLE and Shellshock vulnerabilities. Source: http://www.theregister.co.uk/2014/10/17/apple_releases_mega_security_patch_round_for_osx_server_and_itunes/

October 17, Softpedia – (International) **Modular malware for OS X relies on open-source keylogger code.** Kaspersky Lab researchers identified a piece of modular malware for Apple OS X known as Ventir that uses the legitimate LogKext keylogging software in order to steal information from infected systems. Source: http://news.softpedia.com/news/Modular-Malware-for-OS-X-Relies-On-Open-Source-Keylogger-Code-462473.shtml

October 17, SC Magazine – (International) **Sandworm vulnerability seen targeting SCADA-based systems.** An advisory issued by Trend Micro stated that researchers have identified attackers using the Sandworm vulnerability to target systems running the GE Intelligent Platform's CIMPLICITY human-machine interface (HMI) solution used in supervisory control and data acquisition (SCADA) systems. The attackers appear to be using the vulnerability in the first stage of an advanced persistent threat (APT) targeted attack and use the vulnerability to install the Black Energy malware. Source: http://www.scmagazineuk.com/sandworm-vulnerability-seen-targeting-scada-based-systems/article/377846/

Phone hackers dial and redial to steal billions

NY Times, 20 Oct 2014: Bob Foreman's architecture firm ran up a $166,000 phone bill in a single weekend last March. But neither Mr. Foreman nor anyone else at his seven-person company was in the office at the time. "I thought: 'This is crazy. It must be a mistake,' " Mr. Foreman said. It wasn't. Hackers had broken into the phone network of the company, Foreman Seeley Fountain Architecture, and routed $166,000 worth of calls from the firm to premium-rate telephone numbers in Gambia, Somalia and the Maldives. It would have taken 34 years for the firm to run up those charges legitimately, based on its typical phone bill, according to a complaint it filed with the Federal Communications Commission. The firm, in Norcross, Ga., was the victim of an age-old fraud that has found new life now that

most corporate phone lines run over the Internet. The swindle, which on the web is easier to pull off and more profitable, affects mostly small businesses and cost victims $4.73 billion globally last year. That is up nearly $1 billion from 2011, according to the Communications Fraud Control Association, an industry group financed by carriers and law-enforcement agencies to tackle communications fraud. Major carriers have sophisticated fraud systems in place to catch hackers before they run up false six-figure charges, and they can afford to credit customers for millions of fraudulent charges every year. But small businesses often use local carriers, which lack such antifraud systems. And some of those carriers are leaving customers to foot the bill. The law is not much help, because no regulations require carriers to reimburse customers for fraud the way credit card companies must. Lawmakers have taken the issue up from time to time, but little progress has been made. Last year, Senator Charles E. Schumer, Democrat of New York, pushed the Federal Communications Commission to adopt new regulations after dozens of small businesses around Albany were hit with the swindle. But the agency has not taken any action, and the cause appears to have petered out. Representatives for the agency and the senator's office did not return requests for comment. The scheme works this way, telecommunications fraud experts say: Hackers sign up to lease premium-rate phone numbers, often used for sexual-chat or psychic lines, from one of dozens of web-based services that charge dialers over $1 a minute and give the lessee a cut. In the United States, premium-rate numbers are easily identified by 1-900 prefixes, and callers are informed they will be charged higher rates. But elsewhere, like in Latvia and Estonia, they can be trickier to spot. The payout to the lessees can be as high as 24 cents for every minute spent on the phone. Hackers then break into a business's phone system and make calls through it to their premium number, typically over a weekend, when nobody is there to notice. With high-speed computers, they can make hundreds of calls simultaneously, forwarding as many as 220 minutes' worth of phone calls a minute to the pay line. The hacker gets a cut of the charges, typically delivered through a Western Union, MoneyGram or wire transfer. In part because the plan is so profitable, premium rate number resellers are multiplying rapidly. There were 17 in 2009; last year there were 85, according to Yates Fraud Consulting, which is based in Britain. In 2012, hackers hijacked the phone lines at 26 small businesses around Albany and ran up phone bills as high as $200,000 per business over the course of a few days. Those businesses that contracted with major carriers received credit that covered much of the fraud, though some ended up paying a few thousand dollars. Those who had signed up with a local carrier, Tech Valley Communications, were not so lucky. Tech Valley sued three of its clients to pay huge bills, according to court filings. Best Cleaners, a dry cleaning chain that operates in three states, was one victim. At that business, hackers placed more than 75,000 minutes of premium calls, totaling $147,000. At American Energy Care, a small consulting firm in Albany, the bill reached $200,353. A billboard advertising business in Cohoes, N.Y., was charged $18,000. All settled their cases with Tech Valley. None would discuss the case because of the terms of the settlement, but Best Cleaners said the cost was enough to force it to cancel a planned expansion. Industry groups are trying to tackle the problem but say it is hard to keep up with. Roberta Aronoff, the executive director of the Communications Fraud Control Association, said she routinely loads fake "hot numbers" into a fraud management system, sharing them with carriers so they can be blocked. Catching the criminals is difficult because the crime can cross as many as three jurisdictions. In 2011, the Federal Bureau of Investigation and police in the Philippines arrested four men who used the scheme to make $2 million in fraudulent calls; revenue was directed to a Saudi Arabian militant group that United States officials believe financed the 2008 Mumbai terrorist bombings. Foreman Seeley Fountain, the architecture firm, is disputing its $166,000 bill with its carrier, TW Telecom. The bill now includes $17,000 in late charges and termination fees. To read more click **HERE**

Staples investigating possible data breach

AP, 21 Oct 2014: Staples is looking into a potential credit card data breach and has been in touch with law enforcement officials about the issue. The office supplies retailer said Tuesday that if it turns up any data discrepancies during its investigation, customers won't be responsible for fraudulent activity on their credit cards as long as it is reported in a timely manner. "We take the protection of customer information very seriously, and are working to resolve the situation," spokesman Mark Cautela said in a statement. Earlier

this month Sears Holdings Corp. reported a breach at its Kmart stores that started last month, saying some customers' credit and debit cards may have been compromised. Other breaches have occurred at retailers including Target Corp., Supervalu Inc. and Home Depot Inc. To read more click HERE

Intel Launches Thumb Drive-Sized PC with Windows 8.1

SoftPedia, 20 Oct 2014: We've heard of Windows 8.1's ability to install a fully working, bootable version of itself on USB flash drives, but we haven't seen many examples of it, so Intel has decided to provide one. To be fair, anyone who owns a copy of the OS can make a bootable USB drive, so it's not quite such a big deal. Probably why Intel didn't even bother releasing a PR about it. Still, stealth release or no, the new Meegopad Windows HDMI TV stick differs from the norm because of just that: it's an HDMI stick, not a USB stick. So it's a sort of mini PC / media player device in the shape of a thumb drive the size of a USB stick. Inside, you have a quad-core 1.83 GHz Intel Atom Z3735F processor with 2 MB cache, 16 GB or 32 GB eMMC storage space, 1-2 GB of DDR3 RAM, a microSD card slot, two micro USB 2.0 ports, Bluetooth 4.0, and Wi-Fi (802.11n). A power button is located on the outer shell. As for software, there's not much pre-loaded other than the OS. Speaking of which, you can have it loaded with Android or Linux if Windows 8.1 isn't your thing. The price is of $110 / €110, plus $14.5 / €14.5 more if you want 2 GB instead of 1 GB RAM. To read more click HERE

Keylogger in Phishing Email Also Takes Screenshots

SoftPedia, 20 Oct 2014: A malicious email claiming to come from the HSBC financial institution has been found to deliver a keylogger that can not only intercept keystrokes and the name of the windows they are entered in, but also take pictures of the victim's desktop screen. The malware is also equipped with the ability to steal passwords stored in the web browser, as well as several other programs, and sends all the data to the attackers in real time. Ronnie Tokazowski of PhishMe caught a sample of the email and proceeded to dissect the malicious file in it. After analyzing the keylogger, he determined that the piece was written in .NET and that the coder was ill-prepared for the task, since the researcher managed to easily intercept the data seeping out of the infected machine, as well as identify the communication method with the attacker. Tokazowski observed that the malware was sending emails via SMTP (Simple Mail Transfer Protocol) over port 587, and that the attacker hard-coded the authentication password in the malware. By including the credentials to their command and control email into the malware binary, the attackers run the risk of having someone break into their inbox and remove all the information received from the victims. Not only this, but the researcher also allowed pictures of the screen to be taken when he was intercepting the traffic generated by the malware. In a "watching you watching me" scenario, he saw how screens with his analysis of the traffic were sent over. This particular malicious sample is not new, and it has been found on Hack Forums, a platform used by both white hats and hacker wannabes for ready-made resources. Posters there referred to it as Dynasty Keylogger or as Predator Dynasty. The email body is simple in construction and only informs the recipient that a payment file has been attached, as per the request of the owner of the banking account. This could be sufficient to fool numerous unsuspecting users to check deeper into the matter. As soon as the attachment is deployed, the keylogger is installed on the computer and starts its activity. Generally, keyloggers are integrated as a component of a malware package with different functionality, such as the one recently discovered by Kaspersky targeting machines running OS X. In that case, the attackers relied on an open-source tool to capture keystrokes. A more interesting method to harvest log-in details was observed last week, when a phishing page for Dropbox was hosted in a Dropbox account, allowing the crooks to take advantage of the SSL connection to prevent ringing the alarm bells of the potential victim. To read more click HERE

National Domestic Workers Alliance Suffers Email System Breach

SoftPedia, 20 Oct 2014: The National Domestic Workers Alliance (NDWA) announced that an unauthorized intrusion on its email system led to exposing personally identifiable information and financial details of some of its employees. NDWA is an organization that promotes state and national laws seeking standardization of domestic worker legislation in the US. On Thursday, the group started to inform

affected individuals about the incident, providing instructions on how they can protect against identity theft or fraud on their banking accounts. "The types of personal information that may be contained in the email accounts include social security numbers, deposit account numbers and insurance enrollment information," reads the letter to the people impacted by the intrusion, signed by Tara Ellison, finance and operations director. As soon as they learned about the unauthorized activity, NDWA initiated a forensics investigation to determine whether personal details have been accessed, but the investigators were unsuccessful in the task. However, since the risk of exposure exists, individuals are advised to notify the bank holding the account about the incident and to place a "fraud alert." As a result of this, getting credit in the name of the victim would be more difficult because minute verification of the request is carried out. Ellison also informs in the letter that a one-year complimentary membership for identity protection services is offered to the employee. To read more click **HERE**

Small Healthcare Facilities Have Little Concern about Losing Patient Data

SoftPedia, 20 Oct 2014: With cyber-attacks and intrusions occurring on a more frequent basis, most small healthcare organizations do not worry too much about failing to protect customer information should such an event happen to them, a study reveals. The research, conducted by CSID, a company offering data breach solutions and proactive response and management against this type of events, showed that most participating healthcare facilities (28.6%) do not have a crisis plan to activate in case of a data breach incident. Despite this, and the fact that they are unprepared to counter such an unfortunate event, 83.3% are not worried about cybercriminals penetrating their systems and accessing information about their customers. Even more, few of them have enabled two-factor authentication (2FA) for the personnel with access to the electronic health records, and do not have a policy for auditing the vendors that have access to patient data. However, it appears that they understood the benefits of having a strong password, but unfortunately, this is far from being an impediment for hackers, who no longer resort to brute-force attacks to obtain access credentials. Their technique has refined and a strong countersign is not providing better security in case of phishing or vulnerabilities in Internet-facing computer systems facing. According to the study, about half of the employees with access to patients' records can also log into the personal email at work, increasing the risk of compromising a company computer or stealing the employees' credentials. Once inside the company network, an intruder could move to sensitive areas of the infrastructure where financial information about the patients is stored. Investment in security measures to proactively mitigate the risk of a breach, is done by only a small number of healthcare units, who spend less than 10% of the entire IT budget for data protection. "With the rise of electronic medical records, one weak link can be devastating for the whole system," said Joe Ross, president and co-founder of CSID. Furthermore, among the findings of the study is the fact that these organizations lack the appropriate resources and knowledge to keep the information about their patients safely stored on their systems. The risk is not only for the patients, since the company responsible with safeguarding sensitive details about them also records financial losses; these occur in the wake of a compromise and take the form of forensic investigation as well as identity theft services offered to individuals affected by a potential breach "It is going to be increasingly important for all healthcare facilities to proactively protect against medical data theft by implementing stronger security protocols and having a breach plan in place," said Ross. To read more click **HERE**

JP Morgan Hackers Attacked at Least 13 Other US Financial Institutions

SoftPedia, 10 Oct 2014: More than a month after the cyber-attack against JP Morgan Chase has been disclosed, the investigation reveals that the financial institution was not the only one sighted by the hackers and that at least 13 other banks were attacked. The fact that other financial organizations were targeted by the malicious actors was known from the beginning, but the investigation did not reveal the number of the potentially affected entities, or their names. In a recent report on the matter, Bloomberg revealed some of the institutions that were impacted by the incident, either through successful penetration or just through an attempt that was deflected by the intrusion prevention systems. It appears that among the potential victims are Citigroup Inc., HSBC Holdings Plc (HSBA), E*Trade Financial Corp.

(ETFC), Regions Financial Corp. (RF), and Automatic Data Processing Inc. (ADP). There is no confirmation that their systems were breached, but in some cases, the malware managed to find its way on inside computers. Traces of the threat were also found in the logs of the devices guarding the organization's infrastructure. As the JP Morgan investigation developed, more and more interesting details started to appear. At the beginning, it was revealed that the company systems had been infiltrated a couple of months before the attack was detected and that the operators behind it probed the systems in search of a weak spot, which was later exploited through custom tools. The company also disclosed that 90 servers were breached and personal information of 83 million customers was exposed, although no financial data leaked. A few days back, New York Times reported that the number of financial institutions targeted in this campaign was larger than it was previously suspected, 10 organizations being impacted. With the latest information from Bloomberg saying that the total has now risen to 14, individuals close to the investigation are not sure that this is the final number, as the list may grow. "It's frankly not surprising that there are at least 13 other financial services companies that were targeted by the attackers that broke into JPMC. Data is the new currency, and clever thieves have figured out how to breach the perimeter security measures most companies have relied on," said Michele Borovac, VP at HyTrust via email. There is a strong belief that this will happen, as financial companies complete their own internal investigation and determine the signs of intrusion or compromise sent out by the Financial Services Information and Analysis Center. As far as the identity of the attackers is concerned, there are some leads that the investigators are following. At the moment, there is no solid evidence, but clues point to individuals from Russia, with at least vague connections to government officials. To read more click **HERE**

JP Morgan Chase Cyber-Attack Authors Still Unknown, Russia Ruled Out for Now

SoftPedia, 21 Oct 2014: There has been speculation about the Russian government directing the cyber-attack against JP Morgan Chase this summer, but the FBI denied any indication that the country was involved in the incident, although the possibility has not been ruled out completely. Initially, officials in the investigation told reporters that the suspected reason of the attack was retaliation from the Eastern European country as a result of the sanctions it faced from the Western government because of the conflict in Ukraine. FBI has a different theory, does not confirm government involvement There was no proof at that moment, nor is it now, to support this kind of allegations. However, clues have been found, pointing that the attackers are of Russian origin and have at least some vague connections to government officials. At an event hosted on Monday by the Financial Services Roundtable (FSR), FBI Cyber Division Assistant Director Joseph M. Demarest told Washington Post that the intruders may do some work for the Government, but they also carry out criminal activities on their own. "They may be working as criminals by evening or dark of night and then during the day they're working on behalf of some government," he told the Washington Post. This would explain the complexity of the intrusion, which exploited a zero-day vulnerability and has been found to have lasted for two months before being detected, making it appear a state-sponsored job. The FBI Assistant Director said that it was still early to determine without any doubt who was behind the attack, and that discovering this information takes time, international partners being engaged in the investigative efforts, too. In late August, news about JP Morgan Chase's network being hacked made the rounds on the Internet, more details being revealed as the investigation progressed. In a Securities and Exchange Commission (SEC) regulatory filing, the financial institution disclosed that the amount of affected customers was 83 million, most of them (76 million) being households. Investigation details leaked to the press inform that the cybercriminals managed to access data on more than 90 servers, in some cases, information about the type of customer account (business or mortgage) being exposed. Furthermore, it appears that customer personal information like names, addresses, phone numbers, and email addresses was exfiltrated, along with a list of applications and programs installed on standard JP Morgan computers. However, the databases containing financial information remained untouched, according to the company. This is particularly important to note because the digital assets need to be replaced, an operation that takes both time and effort; but it needs to be done before the cybercriminals find vulnerabilities and leverage them to gain access to the systems. To read more click **HERE**

Feds urge early cooperation in malware investigations

FCW, 20 Oct 2014: The financial services industry has garnered a reputation among cybersecurity professionals for being among the more resilient sectors in the face of cyberattacks. Though the recently publicized hack of J.P. Morgan was a fresh reminder that financial services are always in the crosshairs of cyber criminals, the sector's information-sharing center has been praised for building resiliency against threats. Law enforcement officials made the case at an Oct. 20 conference on cybercrime that this resiliency was due, in part, to public-private cooperation and aggressive federal prosecution of cybercriminals. "This is the new normal for the United States government," declared FBI Executive Assistant Director Robert Anderson, the bureau's top cyber official, after rattling off recent Justice Department prosecutions of cybercriminals. Speakers at the conference hosted by the Financial Services Roundtable in Washington, D.C., tried to answer a common question from the private sector: Who do you call in the government when your firm has been hacked? A succinct answer was not forthcoming, though speakers implied that as long as one of a handful of agencies in the departments of Homeland Security or Justice is notified, the government's response to the incident would be coordinated. "Now I feel quite confident that if you just have a good, solid government point of contact … in cyber, you're going to get the right people in the room, and that's because our cyber centers are in lockstep," said Jason Truppi of the FBI's Major Cyber Crimes Unit. Ari Baranoff, assistant special agent in charge in the Secret Service's Criminal Investigative Division, offered an example of what this "whole-of-government" approach to a cyber breach looks like. The Secret Service got word in July that a small store in Syracuse, N.Y., was the source of a significant amount of credit card data theft, Baranoff said. Two Secret Service agents trained in cyber forensics visited the store, found malware on its server and removed it. The agency then did some "reverse engineering" with the help of Chicago-based firm Trustwave to determine that the malware was original and not well-known to security professionals. The DHS Computer Emergency Readiness Team issued an alert to industry based on that analysis of the "Backoff" point-of-sale malware. Upon seeing the CERT notice, the UPS Store realized that it had had the same malware on its system for months, according to Baranoff, and the firm was able to limit the malware's spread as a result. To read more click **HERE**

U.S. national security prosecutors shift focus from spies to cyber

Reuters, 21 Oct 2014 - The U.S. Justice Department is restructuring its national security prosecution team to deal with cyber attacks and the threat of sensitive technology ending up in the wrong hands, as American business and government agencies face more intrusions. The revamp, led by Assistant Attorney General John Carlin, also marks a recognition that national security threats have broadened and become more technologically savvy since the 9/11 attacks against the United States. As part of the shift, the Justice Department has created a new position in the senior ranks of its national security division to focus on cyber security and recruited an experienced prosecutor, Luke Dembosky, to fill the position. The agency is also renaming its counter-espionage section to reflect its expanding work on cases involving violations of export control laws, Carlin confirmed in an interview. Such laws prohibit the export without appropriate licenses of products or machinery that could be used in weapons or other defense programs, or goods or services to countries sanctioned by the U.S. government. "We need to develop the capability and bandwidth to deal with what we can see as an evolving threat," said Carlin, who was confirmed to his post in April. As Carlin builds his team, he has also recruited a new deputy, Mary McCord, from the U.S. Attorney's office in Washington. The result, according to experts, could be an uptick in the number of national security-related cases brought in federal court, a shift in focus from the National Security Division's prior mandate to investigate intelligence violations. "This is not just a reshuffling of the deck," said former national security cyber crime prosecutor Nicholas Oldham, who is now in private practice. The changes come amid reports that hackers in Russia and elsewhere are targeting everyone from the North Atlantic Treaty Organization and the European Union, to JPMorgan Chase & Co and other financial institutions. The counter espionage section, which deals less with on-the-ground spies than it used to, will now be called the Counter Intelligence and Export Controls Section. A network of terrorism prosecutors around the country called the Anti-Terrorism Advisory Council, or ATAC, will also be renamed the National

Security/ATAC network to make clear its broader responsibilities, Carlin said. In 2012, Carlin helped create a similar network of national security cyber specialists in each U.S. Attorney's office around the country. That was the first of his efforts to start building cyber expertise within the group of prosecutors that had access to national security intelligence information. In the first public case to come out of the effort, the agency charged five Chinese military officers in May, accusing them of hacking into U.S. nuclear, metal and solar companies to steal trade secrets. The move ratcheted up tensions between the two countries. "This prosecution raises the risk that other countries are going to go after our employees ... it's a risky strategy, but a bold one," said Amy Jeffress, a former national security prosecutor who is now in private practices at Arnold & Porter. While the Chinese officers are not expected to be extradited to face charges in the United States, Carlin said his team is busy with similar cases that would likely be litigated in court. "I think you will more regularly see the use of the criminal justice system ... We are now actively investigating a variety of nation-state cases. Not all, but some, will result in prosecutions," he said. To read more click **HERE**

Hacking ATMs: No Malware Required

GovInfoSecurity, 21 Oct 2014: At last week's Black Hat Europe conference in Amsterdam, Russian penetration-testing experts Alexey Osipov and Olga Kochetova described how they tested the attack method on several ATMs. They say they successfully programmed a credit-card-sized Raspberry Pi computer, which can be connected to the inside of an ATM, for use as a "hardware sniffer" as well as a malicious controller. The device can, for example, intercept PIN codes, as well as send directions directly to different components inside the ATM enclosure, telling them to dispense cash or open the safes in which the cash is stored. The recent rise in ATM malware attacks has led to warnings from law enforcement agencies that ATM operators must beef up the physical security of their money machines. The LINK Scheme, for example, which is the U.K.'s interbank network of ATMs operators, maintains physical security recommendations for ATM operators, and recommends a variety of countermeasures that could help thwart malware - or the proof-of-concept Raspberry Pi attacks. Those include replacing the default locks issued by most vendors and monitoring ATMs with cameras. The researchers' proof-of-concept attack relies, in part, on a set of standard programming interfaces, or APIs, that are built into most ATM host computers and components, including text displays, card readers, PIN pads and the dispenser units. These APIs are known as XFS - which stands for "extensions for financial services" - and are used by many manufacturers' components to communicate with each other. By using these APIs, however, an attacker could bypass the ATM's own host computer, and communicate directly with the different peripherals installed inside the ATM enclosure, Osipov tells Information Security Media Group, speaking on the condition that his employer not be identified. Likewise, any vulnerabilities present in the ATM's operating system might also be exploited. The researchers chose the Raspberry Pi computer for the testing of the ATM hacking technique, Ospirov says, because "we wanted something small that we could add to an ATM and it would work within it, and [to] give ... financial IT security guys the knowledge that some device could be inserted into ATMs in such a way that it won't be noticed by the service engineers who exchange cassettes." The Russian researchers ran their tests on an ATM machine they purchased from a smaller ATM manufacturer, as well as machines for which they'd been hired - by ATM operators - to conduct penetration testing. While the researchers say they have disclosed related vulnerabilities directly to ATM manufacturers, they declined to specify the machines they tested, or the vendors involved. But they noted that one vendor replied that because it was no longer producing the vulnerable piece of hardware, it didn't plan to issue a related fix, despite the hardware still being used in the field. Before a computer can be installed inside an ATM, however, an attacker needs to gain physical access to the enclosure itself, and then plug their device into an Ethernet, USB or RS-232 port. But as recent malware attacks in Eastern Europe and Western Europe have shown, criminals are getting better at not just locating unattended ATMs, but also procuring the keys required to access ATM enclosures, plugging in a USB drive that installs malware on the targeted system, and then rapidly dispensing as much money as possible. To read more click **HERE**

Chinese state accused of attacking Apple's iCloudApple's cloud

TheGuardian, 20 Oct 2014: iCloud users in China are the target of a "man in the middle" attack, most likely run by the Chinese state on connections passing into and out of the country, surveillance experts say. The attack on the storage service began on Monday, the same day the iPhone 6 and 6 Plus were released in China for the first time. It intercepts data passed between the user and iCloud.com, Apple's cloud computing service, by routing all communication between the two through a malicious third party. Typically, iCloud.com employs the SSL internet security protocol to establish a secure connection. To get around that, the Chinese attacker has used a self-signed certificate, which is enough to trick users of insecure browsers into thinking they've accessed the iCloud website through a secure connection. "This is clearly a malicious attack on Apple in an effort to gain access to usernames and passwords and consequently all data stored on iCloud, such as iMessages, photos, and contacts", wrote the Chinese internet freedom organisation Great Fire. "If users ignored the security warning and clicked through to the Apple site and entered their username and password, this information has now been compromised by the Chinese authorities. The organisation speculated that the attack "may also somehow be related again to images and videos of the Hong Kong protests being shared on the mainland." SSL, or Secure Sockets Layer, the protocol used to secure iCloud, relies on certificates signed by one of a number of trusted authorities to verify that the site being connected to isn't intercepted by an eavesdropper. The attack made use of a self-signed certificate, which claims to be iCloud.com but isn't supported by a trusted third party. Most modern secure browsers will reject such certificates, but notably, 360 Secure Browser, a popular browser developed by Chinese firm Qihoo, does not. The "great firewall" is a notoriously imprecise censorship tool, frequently blocking sites on a piecemeal basis or allowing access for seemingly random periods of time, and the iCloud intercept is no different: the attack only occurs if users visit one particular IP address, meaning that it's possible to simply reload the site and try again. As well as running a secure browser which will reject self-signed certificates, one way users can stay safe against attacks like this is by enabling two-step verification on their accounts. That won't stop any attacker seeing what the target looks at – the equivalent of browsing over their shoulder – but it does mean that if usernames and passwords are stolen, they can't be used to gain access to the compromised account. To read more click **HERE**