THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

2 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 1, Jersey Journal – (New Jersey) **Lost disc with Jersey City Medical Center patient data is finally found, hospital says.** Jersey City Medical Center-Barnabas Health officials reported that a missing CD containing the personal data of patients was delivered by UPS in September after it was sent to an outside firm that reviews medical billing data in June. New Jersey patients were notified that none of their personal information was breached after the CD was delivered still sealed in its original packaging. Source: http://www.nj.com/jjournal-news/index.ssf/2014/10/lost_disc_with_jersey_city_med.html

October 1, V3.co.uk – (International) **Four hackers accused of $100m US military software and gaming IP theft.** Four individuals were indicted for allegedly stealing over $100 million worth of intellectual property from game developers and the U.S. Army including data from yet-to-be-released games and training software used to train helicopter pilots. Two of the accused pleaded guilty and reportedly used a SQL injection attack to steal the usernames and passwords of employees and software developers in order to gain access to the data. Source: http://www.v3.co.uk/v3-uk/news/2373278/four-hackers-accussed-of-usd100m-us-military-software-and-gaming-ip-theft

October 1, Softpedia – (International) **Xsser mRAT, advanced spyware for iOS, discovered.** Researchers with Lacoon Mobile Security identified a new remote access trojan (RAT) for iOS mobile devices dubbed Xsser that targets jailbroken iOS devices and can exfiltrate personal and device data. The researchers believe that Xsser is linked to the Chinese government and targets protestors in Hong Kong. Source: http://news.softpedia.com/news/Xsser-mRAT-Advanced-Spyware-For-iOS-Discovered-460640.shtml

October 1, Softpedia – (International) **High risk vulnerability patched in Joomla.** The developers of the Joomla content management system (CMS) released a patch for version 3.x closing two vulnerabilities including a remote file inclusion (RFI) issue that could allow an attacker to run remote files. Source: http://news.softpedia.com/news/High-Risk-Vulnerability-Patched-in-Joomla-460600.shtml

September 30, The Register – (International) **OpenVPN open to pre-auth Bash Shellshock bug - researcher.** The chief technology officer of Mullvad stated that some configurations of OpenVPN are susceptible to the Shellshock vulnerability if Bash is allowed to run scripts. A proof-of-concept for the issue was identified online. Source: http://www.theregister.co.uk/2014/09/30/openvpn_open_to_shellshock_researcher/

September 30, Softpedia – (International) **Asprox botnet malware sent through fake Viber email notification.** An analysis from Tech Help List identified a new spam campaign utilizing fake Viber emails to attempt to add new bots to the Asprox botnet. The analysis noted that the attackers were using several techniques to hide their malicious activity and avoid analysis by researchers. Source: http://news.softpedia.com/news/Asprox-Botnet-Malware-Sent-Through-Fake-Viber-Email-Notification-460498.shtml

CEO indicted for company's alleged mobile spyware app

IDG News, 29 Sep 2014: The CEO of a Pakistani company has been indicted in the U.S. for selling a product called StealthGenie that buyers could use to monitor calls, texts, videos and other communications on other people's mobile phones, the U.S. Department of Justice said. The indictment of Hammad Akbar, 31, of Lahore, Pakistan, represents the first time the DOJ has brought a criminal case related to the marketing and sale of an alleged mobile spyware app, the DOJ said in a press release Monday. Akbar is CEO of InvoCode, the company selling StealthGenie online. Akbar is among the creators of StealthGenie, which could intercept communications to and from mobile phones, including Apple, Android and BlackBerry devices, the DOJ said. StealthGenie was undetectable by most people whose phones it was installed on and was advertised as being untraceable, the DOJ said. Akbar was charged in U.S. District Court for the Eastern District of Virginia with conspiracy, sale of a surreptitious interception device, advertisement of a known interception device, and advertising a device as a surreptitious interception device. He was arrested in Los Angeles on Saturday and is expected to appear before a magistrate judge in the Central District of California late Monday. "Selling spyware is not just reprehensible, it's a crime," Leslie Caldwell, assistant attorney general in the DOJ's Criminal Division, said in a statement. "Apps like StealthGenie are expressly designed for use by stalkers and domestic abusers who want to know every detail of a victim's personal life -- all without the victim's knowledge." StealthGenie was hosted at a data center in Ashburn, Virginia. On Friday, a federal judge in the Eastern District of Virginia issued a temporary restraining order authorizing the FBI to temporarily disable the website hosting StealthGenie. The StealthGenie.com website remained down on Monday. StealthGenie allowed users to target mobile phone owners and record all incoming and outgoing voice calls, according to the indictment. It also allowed purchasers of the app to call the phone and monitor all surrounding conversations within a 15-foot radius, and to monitor the targeted user's incoming and outgoing email and text messages, incoming voicemail, address book, calendar, photographs and videos. Akbar and his co-conspirators allegedly programmed StealthGenie to synchronize communications intercepted by the app with the customer's account so that the customer could review intercepted communications almost immediately from any computer with access to the Internet, the DOJ alleged. To install the app, a purchaser needed to obtain physical control over the phone to be monitored for only a few minutes. Invocode's target population for marketing the app was spouses, boyfriends and girlfriends who suspected their partners of cheating, the DOJ said. To read more click HERE

Contractors, Expect 72-hour Rule for Disclosing Corporate Hacks

NextGov, 29 Sep 2014: Look for the whole government to take a page from the Pentagon and require that firms notify their agency customers of hacks into company-owned systems within three days of detection, procurement attorneys and federal officials say. Right now, vendors only have to report compromises of classified information and defense industry trade secrets. The trade secret rule is new and covers breaches of nonpublic military technological and scientific data, referred to as "unclassified controlled technical information.” That new reporting requirement kicked in Nov. 18, 2013 and applies to all military contracts inked since. The rule “is impactful in large part because it is one of the first very clear cybersecurity directives," said Anuj Vohra, a Covington & Burling senior associate in the firm’s government contracts practice. "We’ll see more regulations like that among nondefense agencies." He was interviewed Monday evening after an industry event hosted by the law firm and George Washington University. Violating certain breach clauses could mean the end of a company's contract or even being banned from government work entirely. Civilian agencies don’t have a comparable breach mandate, even though there has been a steady stream of high-profile hacks governmentwide over the past few years. Examples include computer breaches at Serco, which handled federal employee retirement investments, and USIS, a private firm that conducts background investigations on many civilian and military personnel. Until there is a uniform rule, there will be unrest within the contracting community over why, for instance, the departments of Defense and Homeland Security have different reporting requirements. George Washington University law lecturer Richard Gray, who also serves as DOD's associate general counsel, said he is hopeful the Pentagon regulation "will be the vehicle for applying some harmonization across all the agencies." He spoke to Nextgov, as an academic, not on behalf of the Pentagon, after Monday's event. The controlled unclassified rule might provide some consistency and predictability, "even though it's still always going to be an adaptive open dialogue in this space" of cyber policy, Gray said. "Because it's new and we don't really know what we don't know yet." The rule states that within 72 hours of discovering any compromise of unclassified controlled technical information in a company system, the company must disclose which contracts are affected, the location of the leak and a description of the data compromised, among other things -- to the extent they are known at the time. During his public remarks, Gray said the regulation is mainly directed at companies that have been asleep at the switch on basic network hygiene for a long time. Many, if not most, hacking techniques exploit "existing known vulnerabilities for which there are patches" and other simple solutions, he said. "Most of the problems that we see right now are companies that are not taking advantage of stuff that's free, that's available, that's been out there for months, maybe years." Think updating Adobe. Some contract attorneys expect a sharp uptick in efforts to enforce cybersecurity inside contractors' private offices and facilities. Agencies are "ramping up the regulations," Robert Nichols, co-chair of Covington's government contracts practice, said during the event. "You'll see contractors that are suspended or barred for having inadequate systems," Nichols said. They "may face potential false claims liability if they are putting in invoices, saying, impliedly 'We are complying with these standards,' but they are really not." However, he said he does not think the 72-hour rule will be feasible in many situations. To read more click HERE

FBI releases Malware Investigator portal to industry players

ZD Net, 30 Sep 2014: The FBI's Malware Investigator portal will soon be available to security researchers, academics and businesses. As reported by Threatpost (link), the US law enforcement agency's tool is akin to systems used by cybersecurity companies to upload suspicious files. Once a file is uploaded, the system pushes through anti-malware engines to pull out information on the file -- whether it is malicious, what the malware does, and whom it affects. The Malware Investigator analyses threats through sandboxing, file modification, section hashing, correlation against other submissions and the FBI's own entries concerning viruses and malware reports. Windows files and common file types can currently be analyzed, but this will expand to include other file types in the near future. The FBI says that businesses will find this tool particularly useful, stating on the portal's website: "Public and private sector networks are constantly dealing with malware aimed at disrupting operations, stealing information, and/or interfering with daily business. IT professionals must react nimbly to potential issues, but can only make well informed decisions when they can quickly understand the potential threat to their systems." "Public and private sector networks are constantly dealing with malware aimed at disrupting operations, stealing information, and/or interfering with daily business. IT professionals must react nimbly to potential issues, but can only make well informed decisions when they can quickly understand the potential threat to their systems." Speaking at the Virus Bulletin conference in Seattle, the FBI's Jonathan Burns said API access has been granted for businesses that wish to integrate the engine into their platforms, and the personal details of submitters remain undisclosed and private. While the standard portal is currently available to law enforcement, another portal for researchers, businesses and academics will soon be available. To read more click HERE

The FDA takes steps to strengthen cybersecurity of medical devices

FDA.Gov, 1 Oct 2014: To strengthen the safety of medical devices, the U.S. Food and Drug Administration today finalized recommendations to manufacturers for managing cybersecurity risks to better protect patient health and information. The final guidance, titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," recommends that manufacturers consider cybersecurity risks as part of the design and development of a medical device, and submit documentation to the FDA about the risks identified and controls in place to mitigate those risks. The guidance also recommends that manufacturers submit their plans for providing patches and updates to operating systems and medical software. As medical devices become more interconnected and interoperable, they can improve the care patients receive and create efficiencies in the healthcare system.

Some medical devices, like computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. By carefully considering possible cybersecurity risks while designing medical devices, and having a plan to manage system or software updates, manufacturers can reduce the vulnerability in their medical devices. "There is no such thing as a threat-proof medical device," said Suzanne Schwartz, M.D., MBA, director of emergency preparedness/operations and medical countermeasures at the FDA's Center for Devices and Radiological Health. "It is important for medical device manufacturers to remain vigilant about cybersecurity and to appropriately protect patients from those risks." The FDA's concerns about cybersecurity vulnerabilities include malware infections on network-connected medical devices or computers, smartphones, and tablets used to access patient data; unsecured or uncontrolled distribution of passwords; failure to provide timely security software updates and patches to medical devices and networks; and security vulnerabilities in off-the-shelf software designed to prevent unauthorized access to the device or network. The FDA has neither an indication that specific devices or systems have been purposely targeted, nor reports that any patients have been harmed as a result of cybersecurity breaches, but remains concerned about device-related cybersecurity vulnerabilities and their potential to adversely impact public health. The FDA has been working closely with other federal agencies and the medical device industry to identify and communicate with stakeholders about vulnerabilities. The agency is planning a public workshop this fall to discuss how government, medical device developers, hospitals, cybersecurity professionals, and other stakeholders can collaborate to improve the cybersecurity of medical devices and protect the public health. To read more click HERE

DARPA seeks ideas on cyber vulnerabilities and recoveries

FCW, 1 Oct 2014: The Innovation Information Office (I2O) at DARPA is interested in research on near-term cybersecurity threats and new resiliency strategies. Cyber criminals enjoy a target rich environment (pun intended), but the Defense Advanced Research Projects Agency is hoping to make that a little less true. Two recent solicitations from DARPA invite researchers to peer into the future, to look at what defense and resiliency will look like when strong defensive measures are able to thwart most known attack methods, and adversaries look to exploit a new class of vulnerabilities. The first, a $53 million solicitation dubbed Space/Time Analysis for Cybersecurity (STAC), looks at the possibility of adversaries probing what they call "algorithmic resource usage vulnerabilities," essentially weaknesses in algorithms that allow a smart and determined opponent to discover vulnerabilities for attack – either to disrupt and overwhelm a system or snoop on unintended data leaks. Monitoring these kinds of weaknesses is highly complex and resource intensive. DARPA is looking for automated solutions that allow for human analysts to review millions of lines of code per hour. DARPA is also looking to shore up existing military systems with a $52 million solicitation for Cyber Fault-Tolerant Attack Recovery (CFAR). Pointing out that military systems can fall prey to long-standing, undetected security flaws, DARPA wants ideas on methods for making the work of adversaries more difficult by creating " revolutionary breakthroughs in defensive cyber techniques that can be deployed to protect existing and planned software systems in both military and civilian contexts without requiring changes to the concept of operations of these systems," per the solicitation. To read more click HERE

The Unpatchable Malware That Infects USBs Is Now on the Loose

Wired, 2 Oct 2014: It's been just two months since researcher Karsten Nohl demonstrated an attack he called BadUSB to a standing-room-only crowd at the Black Hat security conference in Las Vegas, showing that it's possible to corrupt any USB device with insidious, undetectable malware. Given the severity of that security problem—and the lack of any easy patch—Nohl has held back on releasing the code he used to pull off the attack. But at least two of Nohl's fellow researchers aren't waiting any longer. In a talk at the Derbycon hacker conference in Louisville, Kentucky last week, researchers Adam Caudill and Brandon Wilson showed that they've reverse engineered the same USB firmware as Nohl's SR Labs, reproducing some of Nohl's BadUSB tricks. And unlike Nohl, the hacker pair has also published the code for those attacks on Github, raising the stakes for USB makers to either fix the problem or leave hundreds of millions of users vulnerable. "The belief we have is that all of this should be public. It shouldn't be held back. So we're releasing everything we've got," Caudill told the Derbycon audience on Friday. "This was largely inspired by the fact that [SR Labs] didn't release their material. If you're going to prove that there's a flaw, you need to release the material so people can defend against it." The two independent security researchers, who declined to name their employer, say that publicly releasing the USB attack code will allow penetration testers to use the technique, all the better to prove to their clients that USBs are nearly impossible to secure in their current form. And they also argue that making a working exploit available is the only way to pressure USB makers to change the tiny devices' fundamentally broken security scheme. "If this is going to get fixed, it needs to be more than just a talk at Black Hat," Caudill told WIRED in a followup interview. He argues that the USB trick was likely already available to highly resourced government intelligence agencies like the NSA, who may already be using it in secret. "If the only people who can do this are those with significant budgets, the manufacturers will never do anything about it," he says. "You have to prove to the world that it's practical, that anyone can do it…That puts pressure on the manufactures to fix the real issue." Like Nohl, Caudill and Wilson reverse engineered the firmware of USB microcontrollers sold by the Taiwanese firm Phison, one of the world's top USB makers. Then they reprogrammed that firmware to perform disturbing attacks: In one case, they showed that the infected USB can impersonate a keyboard to type any keystrokes the attacker chooses on the victim's machine. Because it affects the firmware of the USB's microcontroller, that attack program would be stored in the rewritable code that controls the USB's basic functions, not in its flash memory—even deleting the entire contents of its storage wouldn't catch the malware. Other firmware tricks demonstrated by Caudill and Wilson would hide files in that invisible portion of the code, or silently disable a USB's security feature that password-protects a certain portion of its memory. "People look at these things and see them as nothing more than storage devices," says Caudill. "They don't realize there's a reprogrammable computer in their hands." In an earlier interview with WIRED ahead of his Black Hat talk, Berlin-based Nohl had said that he wouldn't release the exploit code he'd developed because he considered the BadUSB vulnerability practically unpatchable. (He did, however, offer a proof-of-concept for Android devices.) To prevent USB devices' firmware from being rewritten, their security architecture would need to be fundamentally redesigned, he argued, so that no code could be changed on the device without the unforgeable signature of the manufacturer. But he warned that even if that code-signing measure were put in place today, it could take 10 years or more to iron out the USB standard's bugs and pull existing vulnerable devices out of circulation. "It's unfixable for the most part," Nohl said at the time. "But before even starting this arms race, USB sticks have to attempt security." Caudill says that by publishing their code, he and Wilson are hoping to start that security process. But even they hesitate to release every possible attack against USB devices. They're working on another exploit that would invisibly inject malware into files as they are copied from a USB device to a computer. By hiding another USB-infecting function in that malware, Caudill says it would be possible to quickly spread the malicious code from any USB stick that's connected to a PC and back to any new USB plugged into the infected computer. That two-way infection trick could potentially enable a USB-carried malware epidemic. Caudill considers that attack so dangerous that even he and Wilson are still debating whether to release it. To read more click HERE

Data Breach on Flinn Scientific Server Lasted for Four Months

Softpedia, 2 Oct 2014: Cybercriminals managed to infiltrate malware on the web server hosting Flinn Scientific's online store and exfiltrated customer payment information since May 2, this year. Located in Batavia, IL, Flinn Scientific is a prominent provider of science education supplies for students and teachers alike, as well as safety equipment for conducting science experiments in class. The unauthorized access to the computer system storing payment information was discovered on September 8, when the company proceeded to remove the malicious software and started monitoring the machine to make sure that customer data is safe from illegal access. There is no information on the method used by the attacker to plant the malware, but an investigation determined that the details exposed included payment card number, card verification code, expiration date, name, address, and email address. Flinn Scientific started delivering letters to customers that made one or more purchases through the website during the four-month duration of the breach, assuring that additional security measures have been installed to close the door on the vulnerability that allowed compromising the web server. To read more click HERE

Supervalu Suffers New Payment Data Breach

Softpedia, 30 Sep 2014: A little over a month after announcing a compromise of its systems processing card information, Supervalu comes out with a new data breach disclosure, saying that some of its Shop 'n Save, Shoppers Food & Pharmacy and Cub Foods owned and franchised stores have been affected. On August 15, Supervalu revealed that the payment systems at 180 of its locations had been compromised since June 22 through July 17, sensitive information being exposed, such as account numbers, expiration date and/or cardholder's name. Previous security upgrade may have prevented collection of data The recent cyber-attack is believed to have started in late August or early September. The company says that a different malware has been used than in the previous incident; no evidence has been found of a connection between the two incidents. "Upon recognition of this intrusion, the Company took immediate steps to secure the affected part of its network and believes it has eradicated the malware. An investigation of this recently discovered incident is underway," a statement from Supervalu Inc. informs. The security measures implemented after the previous attack appear to have paid off, since the company believes that the technology limited the malware's ability to collect information from payment cards. In fact, until the investigation is complete, there are no details to point to the fact that any card details have been collected in any of the affected stores, other than those at some checkout lanes at four Cub Foods franchised stores. Farm Fresh or Hornbacher's stores along with the Save-A-Lot locations also seem to be safe from the attack. The authorities have been informed of the cybercriminal attempt and an investigation has been started into the matter, with full cooperation from the company. President and CEO Sam Duncan said that although a round of security upgrades has been added to the Supervalu systems in the wake of the previous attack, the company will not stop investing in enhanced protective technology. Four franchised Cub Foods stores in Hastings, Shakopee, Roseville (Har Mar) and White Bear Lake, Minnesota, were affected by the incident because they did not benefit from the upgrades implemented after the previous breach. Data exposed at these locations consists of account numbers, as well as the expiration date in some cases. Other numerical information and/or the cardholder's name have also been put at risk. August 27 is given as the earliest start date for the intrusion, which lasted all through September 21, at the latest. To read more click HERE

FBI Warns of Possible Cyber Retaliation in Response to Airstrikes in Iraq and Syria

Softpedia, 30 Sep 2014: As a result of the military actions taken against Iraq and Syria, the FBI notifies of a potential cyber response from the ISIS (Islamic State of Iraq and al-Shams) group and its supporters. The group is also known as the Islamic State of Iraq and the Levant (ISIL) and the Islamic State (IS). At the moment, there is no information about hacktivist groups supporting the ISIS ideology preparing for such activity, so the document from the FBI Cyber Division is a cautionary one. The file is aimed at the private industry and law enforcement and has at its origin intelligence gathered from social media platforms, Twitter included, since the beginning of the year. Although the threats are "nonspecific, and probably aspirational," their iteration has been observed during early September. "As of early-September 2014, a British media outlet identified the hacker known as Aby Hussain Al Britani as a Syria-based ISIL fighter. Al Britani previously served a six-month sentence in the United Kingdom for hacking the e-mail account of former Prime Minister Tony Blair," the FBI document says. Furthermore, the Bureau noticed a tweet from user @Dawlamoon, instigating against Twitter employees, probably because the microblogging company took down several pro-ISIL accounts. Fear of a cyber-attack under the current military conditions is not unfounded, as hacktivist groups and extremist cyber actors have targeted the websites of US organizations, commercial and governmental, in the past, as a response to military actions in the Middle-East or foreign policies for the region. The attacks could come under the form of cross-site scripting (XSS), Structured Query Language (SQL) and service disruption through DDoS (distributed denial-of-service) attempts. The document provides instructions for defending against these types of attacks that could lead to infiltration into sensitive areas of a company or organization in order to exfiltrate information and steal personal details. Setting up or revising a data backup plan to store the data in secure locations so that it can be easily restored is the first measure on the FBI's list. DDoS mitigation strategies are also recommended by the FBI, along with implementation of monitoring systems that can record the activity during a potential attack. Phishing is known to be a powerful tool, especially in targeted attacks that leverage personal information about the victim; as such, having employees capable of detecting a fraudulent email is particularly important. Apart from these, the Bureau advises using encryption for sensitive data, implementing strong passwords that are changed on a regular basis, employing network monitoring and establishing “a relationship with local law enforcement and participate in IT security information sharing groups for early warnings of threats.” To read more click HERE

Warning: Some iOS 8 Keyboards Are Keyloggers

Softpedia, 1 Oct 2014: Be careful what third-party keyboard you use with your iOS 8 device. A prompt to “allow full access” reveals that the developer of that keyboard has the right to record anything that you type. Apps like SwiftKey will also transmit to their server things that you have already typed on that phone. Scary, to say the least. Of course, developers like SwiftKey are reliable. They state their intentions loud and clear. But other developers may not be so straightforward about their intentions. Apple notes in the App Extension Programming Guide that it’s the developer’s responsibility to refrain from using keystrokes against the user. “A network-enabled keyboard and its containing app can send keystroke data to your server, which enables you to apply your computing resources to such features as touch-event processing and input prediction. If you employ this capability, do not store received keystroke or voice data beyond the time needed to provide text back to the user or to provide features that you explain to the user.” The guidelines then expressly state, “Each keyboard capability associated with network access carries responsibilities on your part as a developer, as indicated in Table 11-2. In general, treat user data with the greatest possible respect and do not use it for any purpose that is not obvious to the user.” iOS 8 is equally clear about the matter. Whenever you download and install a third-party keyboard app that needs server-side processing, you’re required to visit the Settings pane and enable it. When you do that, a prompt appears to accept or deny the implications. This is what it says (emphasis ours): “Allow Full Access for [app name] Keyboards? Full access allows the developer of this keyboard to transmit anything you type, including things you have previously typed with this keyboard. This could include sensitive information such as your credit card number or street address.” While the App Store password prompt is left out of the equation, for obvious reasons, the keyboard does record strokes from other apps, like password managers, task managers, e-wallets, etc. Until they get the necessary updates to avoid these benevolent “keyloggers,” you need to be really careful what information you input using a third-party keyboard in iOS 8. And remember this: regardless of how safe a developer may appear to be, you can never be 100% sure their servers won’t be attacked by hackers. To read more click HERE

[NMCIWG NOTE: External keyboards are also available for BlackBerry handheld phones]