THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

15 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

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

New Benghazi indictment confirms computers with classified information stolen
Fox News, 14 Oct 2014: An indictment Tuesday of a Libyan militant already behind bars for the 2012 Benghazi attack that killed four Americans confirms that computers with sensitive and classified information were stolen from the consulate during the assault. Fox News was first to report in July that at least two computers were stolen from the consulate. While the State Department initially dismissed Fox's report, the new, 18-count indictment against Ahmed Abu Khattala confirms that sensitive and classified information was lost, including the location of the top secret CIA annex. Abu Khattala, 43, the first militant to be prosecuted for the Benghazi violence, had initially been charged with conspiracy to provide support to terrorists, resulting in death. U.S. officials had described that initial, one-count indictment as a placeholder to allow for him to be brought into court and for a grand jury to hear more evidence. The new indictment does not add to the public account of how the attack unfolded but it does include multiple counts that make Abu Khattala eligible for the death penalty if convicted, including murder of an internationally protected person and killing a person during an armed attack on a federal facility. It also accuses him, among other charges, of providing material support to terrorists, malicious destruction of property and attempted murder of an officer and employee of the U.S. The indictment also alleges rocket propelled grenades, AK 47s and semi-automatic assault rifles were used at the consulate, and then mortars at the Annex during the third wave of the assault – a level of firepower that would contradict the administration's initial explanation that a demonstration had simply turned violent. After his capture during a nighttime raid, Abu Khattala was brought to the U.S. aboard a Navy boat where he was interrogated by federal agents. He remains in custody at a detention facility in Alexandria, Virginia. Federal prosecutors have long accused Abu Khattala of being a ringleader of the Sept. 11, 2012, attacks that killed Ambassador Chris Stevens and three other Americans. Attorney General Eric Holder said the new indictment reflects Abu Khattala's "integral role" in the attacks. But the new superseding indictment against Abu Khatallah does not suggest that he was the mastermind of the plot, but rather that he carried out the plan – he always has been described to Fox as the "muscle on the ground." The superseding indictment alleges that Abu Khattala was involved in the two different attacks, hours apart, on the diplomatic compound. The violence was aimed at killing American personnel at the compound and looting the buildings of documents, maps and computers, the Justice Department says. In the first burst of violence on the night of Sept. 11, prosecutors allege, Abu Khattala drove to the diplomatic mission with other militants and a group of about 20 breached the main gate and later launched an attack with assault rifles, grenades and other weapons. That initial attack killed Stevens and communications specialist Sean Smith and set the mission ablaze. Prosecutors say Abu Khattala supervised the plunder of sensitive information from that building, then returned to a camp in Benghazi where a large group began assembling for an attack on a second building known as the annex. The attack on that facility, including a precision mortar barrage, resulted in the deaths of security officers Tyrone Snowden Woods and Glen Anthony Doherty, authorities say. To read more click **HERE**

October 13, KPTV 12 Portland; KPDX 49 Vancouver – (Oregon) **850,000 people potentially impacted by WorkSource Oregon security breach.** The Oregon Employment Department notified 851,322 individuals October 13 who registered with the WorkSource Oregon Management Information System that their information may have been compromised by a security vulnerability. Users were asked to change passwords and re-set security questions while officials continue to investigate. Source: http://www.kptv.com/story/26776035/worksource-oregon-data-breach-affects-850000-people

October 14, Softpedia – (International) **Dropbox denies being hacked, points to third-party services.** Dropbox announced that its servers were not breached after a list of 420 username and password pairs were publicized on Pastebin with a poster claiming that more would be published with Bitcoin donations. The company reported that the information was stolen from other Web services used by the victims, who had identical usernames and passwords for Dropbox. Source: http://news.softpedia.com/news/Dropbox-Denies-Being-Hacked-Points-At-Third-Party-Services-461989.shtml

October 13, Network World – (International) **The snappening: Snapsaved admits to hack that leaked SnapChat photos.** Snapchat's third-party app Snapsaved was hacked involving the release of 500MB of images containing between 90,000 and 200,000 photos and videos due to a misconfiguration in their Apache server. Snapsaved subsequently deleted the entire Web site and database associated with the breach. Source: http://www.networkworld.com/article/2825359/microsoft-subnet/the-snappening-snapsaved-admits-to-hack-that-leaked-snapchat-photos.html

October 10, Securityweek – (International) **Multiple vulnerabilities found in BMC Track-It! help desk software.** Researchers with the Computer Emergency Response Team Coordination Center at Carnegie Mellon University (CERT/CC) and Agile Information Security found that Track-It! version 11.3.0.355, the IT helpdesk solution created by BMC Software, contains three vulnerabilities related to permissions, privileges, and access control, missing authentication for critical function, and an exploitation using blind SQL injection. The company is working on addressing the issues. Source: http://www.securityweek.com/multiple-vulnerabilities-found-bmc-track-it-help-desk-software

October 10, SC Magazine – (International) **New mobile trojan masquerading as Tic-tac-toe game targets Android devices.** Kaspersky Lab researchers found that a Tic-tac-toe game available on Android devices houses the Gomal trojan which allows hackers to record audio from the microphone, steal incoming SMS messages, steal data from the device log, and obtain root privileges, among other things. Good for Enterprise researchers determined that the app was a proof-of-concept app presented at Black Hat 2013 and used only in Samsung Exynos memory access vulnerability, which has since been patched. Source: http://www.scmagazine.com/new-mobile-trojan-masquerading-as-tic-tac-toe-game-targets-android-devices/article/376722/

October 10, SC Magazine – (International) **HP to remove digital signature that code-signed malware.** Symantec discovered that an HP digital certificate was used to cryptographically sign (code-sign) malware shipped through HP products in May 2010. HP will revoke the digital certificate October 21 after researchers found an apparent signature on a four-year-old trojan that may have been included in the software. Source: http://www.scmagazine.com/hp-to-remove-digital-signature-that-code-signed-malware/article/376737/

Microsoft patches two more 0-days actively used by attackers
Heise Security, 15 Oct 2014: With this month's Patch Tuesday, Microsoft has provided patches for several critical vulnerabilities that allow remote code execution, some of which have been or are actively exploited in the wild. We have already written about the SandWorm (CVE-2014-4114), which was used by the homonymous cyber espionage group for targeting NATO, the EU, Ukrainian and Polish government organizations, and European companies in the telecommunications and energy sectors. The vulnerability could allow remote code execution if a user opens a Microsoft Office file that contains a specially crafted OLE (Object Linking and Embedding) object. Another critical update is that for two privately reported vulnerabilities in Microsoft Windows, and the more severe of the two (CVE-2014-4148) also "allows remote code execution if an attacker convinces a user to open a specially crafted document or to visit an untrusted website that contains embedded TrueType fonts." The second one is an elevation of privilege vulnerability (CVE-2014-4113) that is triggered when the Windows kernel-mode driver improperly handles objects in memory. To exploit this vulnerability, an attacker must have valid logon credentials and be able

to log on locally, Microsoft noted in the bulletin. Microsoft is aware of "limited attacks" trying to exploit these two vulnerabilities, but has not named the attackers. According to Symantec, there are reports that CVE-2014-4148 is being used to gain remote access into an international organization. The vulnerability is exploited through a document with a malicious TrueType Font, and delivers a "somewhat sophisticated remote access Trojan (RAT) that would run from memory" onto the targeted computer. CrowdStrike reports that the CVE-2014-4113 vulnerability, which affects all Windows operating systems from Windows 2000 through Windows 7, has been leveraged by Hurricane Panda, "a highly advanced adversary believed to be of Chinese origin and known to be targeting infrastructure companies." For more technical details, check out their blog post. To read more click **HERE**

Microsoft patches SandWorm 0-day

Heise Security, 14 Oct 2014: Microsoft is back in fine form this month with eight upcoming advisories affecting Internet Explorer, the entire Microsoft range of supported operating systems, plus Office, SharePoint Server and a very specific add on module to their development tools called "ASP .NET MVC". Originally nine advisories were listed in the advance notice, but one of the vulnerabilities affecting Office and the Japanese language IME was dropped for reasons unknown (the dropped advisory was bulletin #4 in the advance notice). The big headline this month seems to be SandWorm, another vulnerability being marketed with a clever name. SandWorm, a.k.a. CVE-2014-4114 is addressed by MS14-060. Why is it called SandWorm? Apparently the exploit code was written by a fan of Frank Herbert's classic science fiction epic, Dune. The code and command and control URLs contain references to the books. That's it. Note, SandWorm is not a "worm" in the sense of computer virus that can self-propagate. The average system administrator or home users should not panic about SandWorm. While the reach is pretty broad because the vulnerability in question affects all versions of the Windows operating system from Vista SP2 to Windows 8.1, and Windows Server editions 2008 and 2012, we have to emphasize that this is a local file format exploit. They're a fairly common class of issue and Microsoft patches these kinds of things routinely. It's not what we consider to be truly remotely exploitable. It's not like Heartbleed or ShellShock, where an attacker could just "do" this to a vulnerable system. An attacker needs to launch a multi-stage attack to take advantage of this vulnerability; they need to have already achieved initial compromise through some other method, possibly social engineering. Once they do that, the bug is nasty as it allows an attacker to take complete control of the compromised system, but the steps required to get there limit the impact of this vulnerability. It's worth noting that in the advance notification, Microsoft only called this issue "Important" and patching priority 2, that is, one step down from their most severe ratings and patch urgency. Of the issues in this month's patch that are not SandWorm, three of the advisories, MS14-056, MS14-057, and MS14-058, are rated "Critical", Microsoft's most severe designation based on the impact of exploitation and the likelihood of an exploit emerging, including the IE issue and two issues affecting virtually every supported Operating System. These will be the top patching priorities, probably with the IE issue being the most at risk for exploitation. Behind the three critical, there are four issues marked as Important (including the SandWorm vulnerability, MS14-060), enabling either remote code execution or elevation of privilege. Again, most Windows versions are affected, plus in one case, Office and SharePoint. These will be the second patching priority. In the case of MS14-062, the affected the Message Queuing component is not installed by default and there are no known active attacks. It is worth mentioning that the FAT32 issue, MS14-063, requires physical access to exploit. The most likely scenario here is the passing of a malicious USB device. The issue in ASP .NET MVC, identified by Microsoft as MS14-059, is a security feature bypass and due to the relatively limited exposure of that feature should be addressed on an "if and when" basis. As usual, we recommend updating your Microsoft systems with these patches as soon as possible. To read more click **HERE**

Suspected Russian "Sandworm" cyber spies targeted NATO, Ukraine

ARStechnica, 13 Oct 2014: A group of cyber spies targeted the North Atlantic Treaty Organization (NATO), Ukrainian and Polish government agencies, and a variety of sensitive European industries over the last year, in some cases using a previously unknown flaw in Windows systems to infiltrate targets,

according to a research report released on Tuesday. Dubbed "Sandworm" by iSIGHT Partners, the security consultancy that discovered the zero-day attack, the campaign is suspected to be Russian in origin based on technical details, the malware tools used, and the chosen targets, which also included government agencies in Europe and academics in the United States. If confirmed, the attack is an uncommon look into Russia's cyber-espionage capabilities. "We can confirm that NATO was hit; we know from several sources that multiple organizations in the Ukraine were targeted," said John Hultquist, senior manager of cyber-espionage threat intelligence for iSIGHT. "We have seen them using Ukrainian infrastructure as part of their attacks." The Sandworm Team, named because its members include references from Frank Herbert's Dune series in their code, also used a previously unknown software flaw to compromise some targets. Using the security hole, the Sandworm group could execute their attacks on systems running up-to-date versions of Windows Vista, Windows 7, Windows 8, and Windows RT. Microsoft plans to release a patch for the flaw during its regular updates on Tuesday. "The power of the exploit is pretty substantial," Hultquist said. "From talking to some people over here, they have had a hard time writing signatures for it, and the attack does not crash anything. It's subtle." Ironically, Windows XP, which Microsoft for the most part no longer supports, is not vulnerable to the attack. "We have observed over a hundred individual victims of these campaigns during our monitoring of the botnets," Robert Lipovsky stated in ESET's initial analysis of the campaign in September. Originally created seven years ago as a denial-of-service tool, Black Energy became a popular attack tool for Russian and Eastern European cyber-criminals. The program is not the first to be repurposed for cyber-espionage. An up-and-coming banking trojan named Dyre has become popular as a tool for espionage. The antivirus firms' original analysis did not find signs of the 0day exploit. The attackers made use of a variety of software flaws in addition to the 0day exploit, in some cases chaining together attacks on two vulnerabilities to gain the necessary privileges to run code on the targeted system—an increasingly common practice. The security consultancy tracks at least five apparent Russian groups that focus on cyber espionage. The Sandworm Team targeted NATO as far back as December 2013, while attendees to a global security conference were targeted in May of 2014. In June, a Polish energy firm, a French telecommunications firm, and other critical industries were targeted. To read more click **HERE**

Poor punctuation leads to Windows shell vulnerability

ARSTechnica, 10 Oct 2014: 52 A class of coding vulnerabilities could allow attackers to fool Windows system administrators into running malicious code because of a simple omission: quotation marks. The attack relies on scripts or batch files that use the command-line interface, or "shell," on a Windows system but contain a simple coding error—allowing untrusted input to be run as a command. In the current incarnation of the exploit, an attacker appends a valid command onto the end of the name of a directory using the ampersand character. A script with the coding error then reads the input and executes the command with administrator rights. "The scenario... requires a 'standard' user with access rights to create a directory to a fileserver and an administrator executing a vulnerable script," Frank Lycops and Raf Cox, security researchers with The Security Factory, said in an e-mail interview. "This allows the attacker to gain the privileges of the user running the script, thus becoming an administrator." While the attack falls short of the severity of the Shellshock family of Linux shell vulnerabilities, the two researchers stressed that it's a good example of how untrusted input can be used to execute commands on a system. The researchers identified at least one popular script with the vulnerability. When the script attempts to set the starting directory for system administration work, it inadvertently runs the command appended to the malicious directory's name as well. Another scenario posited by the researchers involves companies that use scripts to copy data from a public network to an internal system. "The attacker might be a potential customer or a supplier," they note, not just a corporate user. The solution is to use proper coding practices—in this case, the judicious use of quotation marks. Quotation marks are used in the shell environment to make sure that the data inside the quotes is not interpreted by the program as a command. Allowing untrusted input to run as a command is one of the "top 25 most dangerous software errors," as determined by the SANS Institute. "In the end, it comes down to input validation, as (it does)

quite often, but it doesn't hurt to stress the importance of it," the researchers said. . To read more click HERE

Algorithms to spot attacks coming from inside the network gets Army support

Computerworld, 14 Oct 2014: When an employee turns on his own company, the results -- damaged networks, data theft and even work stoppage -- could be devastating. It could rock the company even more than an outside attack because the insider knows where sensitive data is kept, what the passwords are and exactly how to hurt the company the most. That's the driving force behind the work that Daphne Yao, associate professor of computer science at Virginia Tech. Yao, who received an NSF Career award for her human-behavior inspired malware detection work, is developing algorithms that will alert companies when an employee might be acting maliciously on their network. And the Army Research Office has awarded her $150,000 to continue her research into finding new ways to detect anomalies caused by system compromises and malicious insiders. "The challenge is to understand the intention of the user and what the user is trying to do," Yao said. "Most are doing legitimate work and they're working their own project and minding their own business. You need a detection system that can guess what the user is trying to do." The crux of Yao's work is to figure out which employees are simply downloading sensitive files or logging onto the network in the middle of the night because they're trying to get their work done and which employees may be doing the same things because they're trying to sell proprietary information or crash the network. According to a 2012 Symantec report, 60% of companies said they had experienced attacks on their systems to steal proprietary information. The most frequent perpetrators were current or former employees or partners in trusted relationships. In 1996, for instance, a network administrator at Omega Engineering Inc. planted a software time bomb that eradicated all the programs that ran the company's manufacturing operations at its Bridgeport, N.J. plant. The trusted IT administrator, Tim Lloyd, effectively stopped the manufacturing company from being able to manufacture, causing the company $12 million in damages and its footing in the high-tech instrument and measurement market. Eighty workers lost their jobs as a result. Lloyd was tried and convicted of computer sabotage in federal court. More recently, in 2013 Edward Snowden leaked classified documents about global surveillance programs that he acquired while working as an NSA contractor. The same year, Pfc. Bradley Manning, an Army intelligence analyst, was sentenced to 35 years for leaking the largest cache of classified documents in U.S. history. These are the kinds of insider attacks Yao is working to stop. The Army Research Office did not respond to a request for comment, but Dan Olds, an analyst with The Gabriel Consulting Group, said he's not surprised that the military is supporting research into detecting insider threats. "The U.S. military is very concerned about security these days," added Olds. "The Bradley Manning leaks highlighted the massive damage that even a lowly Pfc can wreak if given access to a poorly secured IT infrastructure. The Snowden and Manning leaks have had a very severe impact on U.S. intelligence activities, disclosing not only the information gathered, but also showing the sources and methods used to get US intelligence data." He also said insider-based attacks normally may not get as much media attention as most hacks, but can potentially cause much greater damage since the attacker at least knows where the keys to the castle are hidden. And if that attacker works in IT, he or she might even have the keys. "Insider threats are many times the most devastating, as they are the least expected," said Patrick Moorhead, an analyst with Moor Insights & Strategy. "Companies spend most of their security time and money guarding against external threats.... So that sometimes leaves the inside exposed." To combat this, Yao is combining big data, analytics and security to design algorithms that focus on linking human activities with network actions. Typical computer systems monitor things like network traffic, file system events and email activities. They also focus on looking for specific warning signs, like someone uploading large amounts of data. The problem with that is that if someone knows what the warning signs are, they can easily adjust their actions -- uploading data in smaller increments, for instance -- to avoid detection. Yao is taking a different approach; her algorithms are focused on learning what are normal activities and then detecting anything unusual. "We build on a model of normal behaviors and then detect a deviation from normal behaviors," she explained. "If you see a user logging in and access a database or doing a file read or write in the middle of the night..., then you ask, 'Is this a legitimate sequence of actions or is this an anomaly?'"

She also said part of the idea behind her detection system is to corroborate the user's actions with what's happening on the network. If, for instance, a military team is on a reconnaissance mission, then it makes sense that they would be accessing maps from a backend server and pulling various data off the network. It's largely about putting network actions into context. To read more click HERE

Security vendors claim progress against Chinese group that hacked Google

IDG News, 15 Oct 2014: A group of security companies say a collaborative effort has helped counter several hacking tools used by a China-based group most known for provoking strong condemnation from Google four years ago. The companies, which include Cisco, FireEye, F-Secure, iSIGHT Partners, Microsoft, Tenable, ThreatConnect, ThreatTrack Security, Volexity, Novetta and Symantec, said their efforts have led to a better level of protection in their products against the hacking tools used by the group. How long the effort will stymie the hackers remains to be seen. "We're not naïve," said Novetta CEO Peter LaMontagne in a phone interview Tuesday. "Our view is that the threat actors that are out there are absolutely focused on staying ahead of our defensive efforts." Novetta, which spearheaded the effort, said a comprehensive technical report on the action, called "Operation SMN," will be released on Oct. 28., although some details were released by Symantec in a blog post Tuesday. The hackers, referred to as "Hidden Lynx" by Symantec, are believed to have been behind "Operation Aurora," a famous cyberespionage campaign revealed in early 2010 that compromised as many as 20 companies. Google said the attack stole some of its intellectual property and also appeared to target the Gmail accounts of Chinese human rights activists. Google's comments fueled a growing diplomatic row between the U.S. and China over cybersecurity issues. Other U.S. companies followed Google in more directly blaming China for sophisticated long-term infiltration campaigns. In January 2014, Microsoft called for the companies to work more closely together to combat certain types of malware families successfully used by attackers year after year. The project was dubbed the "Coordinated Malware Eradication" program, and its first action took aim at "Hikit," which is a backdoor the Hidden Lynx hackers try to plant on computers. Backdoors allow for probing a compromised computer or for uploading other malware. Hikit has been used against governments and technology, research and defense companies in countries including the U.S., Japan, Taiwan and South Korea, Symantec wrote. The security companies shared information on the group, which has led to "the rollout of more effective protection against Hikit and a number of other associated pieces of malware, including one previously unknown malware tool," Symantec wrote. The Hikit malware was used in a 2012 attack against Bit9, a Waltham, Mass., company that sells a security platform designed in part to stop hackers from installing their own malicious software. Once inside Bit9, the hackers accessed a virtual machine used to digitally sign code for Bit9, a security measure that verifies the company's code is legitimate. The hackers then used Bit9's digital certificate to sign 32 of their own malicious files and scripts, including Hikit. That kind of attack is particularly dangerous. With Bit9's digital signature, Hikit would look legitimate to other security software and not be detected as malware. Further investigation showed HiKit was used in so-called watering hole attacks, where legitimate websites are tampered with to deliver malware to visitors' computers. The Chinese group added more backdoors -- Fexel and Gresim -- to their arsenal in 2013, which were used in conjunction with Hikit. Gresim had remained unknown before the security companies began collaborating, Symantec wrote. To read more click HERE

White House will push piecemeal cybersecurity bills

USA Today, 9 Oct 2014: In an effort to push cybersecurity legislation through Congress, the Obama administration has given up trying to pass one big bill and is opting to break up the legislation into bite-size chunks that lawmakers are more likely to approve, the White House cybersecurity czar said Thursday. "I think it's easier to get smaller pieces through rather than one big cybersecurity bill," said White House Cybersecurity Coordinator Michael Daniel at a news event hosted by the Christian Science Monitor and the Center for National Policy. Daniel said the administration will now focus on "getting whatever we can passed" using whatever legislative vehicle is available. He also acknowledged it will be difficult to make that happen this year, meaning the issue will likely be passed to the new Congress in January. "We

remain committed to (passing legislation)," he said. "Obviously, getting anything passed on Capitol Hill right now is a challenge." The administration is seeking legislation that would make it easier for the Department of Homeland Security to work with private companies to prevent hacker attacks such as the one revealed recently against JPMorgan Chase and nine other U.S. financial institutions. It also wants to increase the agency's legal authority to fight cyberterrorists and allow DHS to hire more cybersecurity professionals to close the security holes that hackers exploit. The House passed a cybersecurity bill earlier this year. The Senate Homeland Security and Governmental Affairs Committee has approved several smaller bills. Homeland Security Secretary Jeh Johnson has been urging Congress to act this year to pass the provisions of cyberlegislation that have bipartisan agreement. In the meantime, President Obama will continue to use his executive authority to improve cybersecurity as much as he is able, Daniel said. To read more click HERE

Hacking a big danger for small businesses

The Washington Post, 8 Oct 2014: It's not just big businesses like JPMorgan Chase, Target and Home Depot that get hacked. Small companies suffer from intrusions into their computer systems, too. The costs associated with computer and website attacks can run well into the thousands and even millions of dollars for a small company. Many small businesses have been attacked — 44 percent, according to a 2013 survey by the National Small Business Association, an advocacy group. Those companies had costs averaging $8,700. JPMorgan Chase said the attack on its computer servers this summer compromised customer information from about 76 million households and 7 million small businesses. Target Corp., Michaels Stores Inc. and Neiman Marcus have also reported breaches of their computer systems in the past year, as did Home Depot Inc., whose customers include small contracting companies. Typically, businesses must have a computer expert find the source of the attack and systems have to be purged of harmful software like viruses. When websites are shut down revenue can be lost. Making matters worse, if customer data was breached, companies often must pay to notify each person or business affected. In some states, they're encouraged to pay for credit report monitoring for customers, says Matt Donovan, head of technology insurance underwriting for the insurer Hiscox USA. In almost every state, companies must notify people when information has been breached, says Samuel Cornish, a commercial law attorney with Genova Burns Giantomasi Webster in Newark, New Jersey. Companies can also be liable for damages in lawsuits brought by customers, he says. AdvertisementSmall businesses are particularly vulnerable to attacks because many owners believe they don't have the time and money to invest in software programs or consulting services to make systems more secure. Many businesses are ignorant of risks they face or possible solutions, says Jeff Foresman, a consultant with Rook Security, an Indianapolis-based computer security company. They may not realize an attack can happen from a seemingly harmless source. For example, a perfectly normal-looking email from a friend's computer that was attacked without the owner's knowledge could lead to trouble. "They don't know what they don't know. They don't understand the sophistication of these attacks," Foresman says. Berkeley Varitronic Systems' bank account was hacked earlier this year and $50,000 was taken, CEO Scott Schober says. He got the money back, but considers the incident a lesson. He had already invested $50,000 in security for his own systems and plans to add another $20,000. Schober believes his Metuchen, New Jersey-based company was attacked via its bank because its business is computer security. "We are a target. Thieves like to send that message," he says. To read more click HERE

Air Force to step up recruiting, shorten training for cyber airmen

Air Force Times, 14 Oct 2014: The Air Force may shorten the training time for cyber airmen to move them into their jobs faster — and airmen with existing cyber certifications would get a head start. The demand for training more airmen particularly at the nine-week intermediate network warfare training course at Hurlburt Field, Florida, is beyond the school's capacity, leaving airmen backlogged, said Air Force spokesman Maj. Eric Badger. The more hands-on training course is required for airmen expected to be part of the U.S. Cyber Command Cyber Mission Force teams, and also for airmen working in advanced operational-level squadrons. "We are taking new actions to recruit cyber-savvy airmen, people with cyber

skills already, and also to shorten the training timeline and to get them into effective roles sooner," said Brig. Gen. Sarah Zabel, the Director, Cyberspace Strategy and Policy, Office of Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force, during a media roundtable at the Air Force Association's Air and Space Conference. Airmen "with existing certifications in network defense or computer defense," Zabel said, will get a head start in training, but other initiatives are also on the table: incorporating more curriculum into initial skills training. Zabel said getting airmen clearances and certifications prior to their training makes an already long process even longer, an unideal situation for a time when protecting cyber networks is crucial to both the Air Force and Defense Department mission. "Cyber is the new wild, wild west," said Gen. John E. Hyten, Air Force Space Command commander in a release. "It took us about 30 years to figure out how to make space a real warfighting domain and operate in it accordingly. We do not have that time in cyber, because cyber is under threat every day." A decision on how the Air Force will reprioritize training for operational units is expected to be made before the end of the year, Badger said. To read more click **HERE**

Tech firms, associations lead response to cybersecurity framework

FedScoop, 14 Oct 2014: The nation's critical infrastructure is massive in its size, diversity and geographic spread literally tens of thousands of financial, transportation, power, telecommunications, manufacturing, health care and government organizations from coast to coast. So it may have been a surprise to some when the National Institute of Standards and Technology posted a mere 53 responses last week to the Obama administration's voluntary framework for improving critical infrastructure cybersecurity. NIST had requested feedback in August from the private sector owners and operators of critical infrastructure to better understand how the framework was being used and how officials might improve the voluntary guidelines in future versions. Although there were several government agencies, and finance and energy companies among the organizations that provided feedback on the framework, the vast majority of responses posted Oct. 10 by NIST came from tech companies and industry associations. "The response was about what I expected," Adam Sedgewick, a senior IT policy adviser who has been leading NISTs work on the cybersecurity framework, said in a telephone interview with FedScoop. "The trade associations represent hundreds of organizations. That's helpful to us because they represent the opinions of broad swaths of industry. And the response is really about how the framework is being used, not about how many have adopted it." Sedgewick said an "initial scrub" of the responses had been completed and there may be more posted on the NIST site. Released in final form in February, the framework is the centerpiece of President Barack Obama's Executive Order 13636 " Improving Critical Infrastructure Cybersecurity " which directed NIST to work with the private sector, which owns and operates more than 85 percent of the nations critical infrastructure, to develop a voluntary set of guidelines and best practices for reducing cyber risks. And while NIST put significant effort into obtaining private sector input during the framework's development, the strategy has been dogged by lingering doubts about how many companies would actually adopt the voluntary standards. Sedgewick, however, said focusing on the number of respondents to the RFI and the number of companies that will adopt the framework is missing the point. The goal, he said, was to learn how they can make the framework better. "We're going to look for certain trends … for example, if standards bodies begin issuing guidance based on the framework," he said. "But understanding adoption rates is really a whole of government responsibility," he said. The Department of Homeland Security did not respond to FedScoop's request for comment. Dell Inc., International Business Machines Corp., Intel Corp. and Microsoft Corp. were among the tech firms that offered responses to the framework. But the biggest response came from an assortment of associations, including the U.S. Telecom Association, Telecommunications Industry Association, CTIA-The Wireless Association, Utilities Telecom Council and the U.S. Chamber of Commerce. Most of the organizations said the framework has been helpful in raising awareness of best practices in cybersecurity risk management. But many of the critical infrastructure vertical industries pointed to existing guidelines and voluntary standards as the centerpiece of their risk management programs and characterized the NIST framework as a supplement that has helped further refine existing standards and processes. To read more click **HERE**