Welcome to the Cyveillance Weekly Trends Report

Greetings from Cyveillance, the leader in open source threat intelligence. Since threat intelligence is constantly evolving, we publish this newsletter to keep our customers updated on the latest threats to various industries. Each week, we'll send you highlights from our analyst research reports. You can unsubscribe at any time. For the latest security news stories throughout the day, you can also follow us on Twitter, or to view the latest security articles from Cyveillance experts, subscribe to our blog.

In this Issue:

- Top Weekly Incidents
- Energy
- Agribusiness
- Insurance
- Financial Services
- Global Intelligence
- Legal and Regulations
- Pharmaceuticals
- Retail
- Technology
- Telecommunications
- Entertainment
- Defense
- Law Enforcement

REGISTER NOW FOR OUR CYBER SECURITY SUMMIT

You’re invited to join us for our upcoming Cyber Security Event October 8 & 9 in Philadelphia, PA, featuring presentations on mobile application security, social media, advanced threats, corporate security, and more. Sign up now to reserve your spot and get more information!
Top Incidents

Energy

- Opponents of the fracked gas pipeline temporarily seized Vermont Gas Systems (VGS) CEO Don Gilbert's 251 Sherman Hollow Road property in Hinesburg on Friday evening through what they called “the people’s eminent domain.” They projected Gas Lands a documentary about the dangers of fracking onto the side of Gilbert's house. Members of Green Mountain EarthFirst! (GMEF!)- the group who organized the event – said the action was meant to highlight the use of eminent domain threatened by VGS in their construction of the fracked gas pipeline in Addison County. "It is a crime for a foreign corporation to take Vermonters’ land without permission and build a fracked gas pipeline that promotes more fossil-fuel consumption and provides 99% of its fuel to an out-of-state paper company” said a member of GMEF!

Agribusiness

- Russia is considering GMO sanctions on all food imports into the country. Experts including scientists and farmers have urged Russian PM Dimitry Medvedev to include GMO's in existing food sanctions on the EU, US, and Australia. The ban would include all 18 varieties of GMO crops approved by Russia with the intention of causing the most economic stress to the EU and US. Monsanto is listed among the largest biotech companies that would be affected.

Insurance/Healthcare

- The quarterly Cloud Adoption and Risk (CAR) Report from Skyhigh Networks uses usage data collected from customers around the world to help explain how some enterprise organizations adopt and use cloud data. Though the High Tech industry led the way with an average of 193 data exfiltration events and 41 malware incidents per quarter, healthcare was next on the list with 63 data exfiltration events and 29 malware incidents. Researchers made the point that, considering how regulated the healthcare and financial industries are, it’s interesting that their risk activities are marginally higher than other non-regulated industries.

Financial Services

- Multiple banks said they were seeing evidence that a leading U.S. retailer of home improvement and construction products and services may be the source of a massive new batch of stolen credit and debit cards that went on sale last week in the cybercrime underground. A leading security researcher said new data gathered from the cybercrime underground suggests that the apparent payment card breach at the company involves nearly all of its stores across the nation. Other industry experts said there are signs that the perpetrators of this apparent breach may be the same group of Russian and Ukrainian hackers responsible for the data breaches at Target, and an Asian-themed US casual dining restaurant chain, among others.

Global Intelligence

- North Korea's cyberwarfare capabilities are on the rise despite being entrenched in aging infrastructure and dampened by a lack of foreign technology. South Korea claims that North Korea's "premier" hacking unit, Unit 121, is behind the US and Russia as the "world's third largest cyber unit." South Korea estimated that North Korea's hacking team comprises of roughly 3000 staff, while a report released by South Korean publication Yonhap upgraded this figure to 5900. However, North Korea maintains heavy restriction on Internet use, which is censored by the state and only used by the social elite, meaning that any attacks originating from the country are highly likely to be state-sponsored, and rogue actors are unlikely to exist.

Legal and Regulations
As of August 22, 373 TLDs have been introduced to the internet, with 1,321 TLDs still proceeding.


**Pharmaceuticals**

- Agora, another online black market is reported to have more product listings than other markets on the dark net after the FBI’s Silk Road bust in 2013. Agora’s biggest advantage is its large user base has attracted a critical mass of drug dealers, who in turn draw more customers.

**Retail**

- A new report claims the apparent data breach at Home Depot could be “much, much bigger” than last year’s infamous Target infiltration. Evidence gathered by security blogger Brian Krebs suggests the breach involves nearly all of Home Depot’s 2,200-plus stores nationwide.

**Technology**

- This week, some of the biggest tech companies will lead a symbolic “Internet Slowdown” to protest the Federal Communications Commission’s network neutrality proposal. “Several top websites—including Etsy, Kickstarter, Foursquare, WordPress, Vimeo, reddit, Mozilla, Imgur, Meetup, Cheezburger, Namecheap, Bittorrent, Gandi.net, StartPage, BoingBoing, and Dwolla—announced that they will be joining more than 35 advocacy organizations and hundreds of thousands of activists in a day of action that will give a glimpse into what the Internet might look like if the FCC’s proposed rules go into effect,” the advocacy group “Fight for the Future” said.

**Telecommunications**

- Rogue cellphone towers have been discovered in the USA. The fake cellphone towers were used by unknown threat actor(s) to eavesdrop mobile communication.

**Defense**

- Ministers are due to ratify NATO’s new cyber defense policy. The new policy means that a digital attack can now be considered as the equivalent of an attack with tanks or rockets and could trigger NATO’s collective defense clause.

**Law Enforcement**

- The Justice Department launched a broad investigation into the police department in Ferguson, Missouri, following recent unrest. The investigation, which is separate from an existing federal probe into the Aug. 9 shooting of Michel Brown, will look for patterns of discrimination within the predominantly white department and focus on how officers use force, search and arrest suspects, and treat inmates at the city jail. The police department said it welcomed the investigation.

**Energy**

- Opponents of the fracked gas pipeline temporarily seized Vermont Gas Systems (VGS) CEO Don Gilbert’s 251 Sherman Hollow Road property in Hinesburg on Friday evening through what they called “the people’s eminent domain.” They projected Gas Lands a documentary about the dangers of fracking onto the side of Gilbert’s house. Members of Green Mountain EarthFirst! (GMEF!)- the group who organized the event – said the
action was meant to highlight the use of eminent domain threatened by VGS in their construction of the fracked gas pipeline in Addison County. "It is a crime for a foreign corporation to take Vermonters’ land without permission and build a fracked gas pipeline that promotes more fossil-fuel consumption and provides 99% of its fuel to an out-of-state paper company” said a member of GMEF!

- Today more than a dozen Bay Area citizens chained themselves to a gate at the Kinder Morgan rail terminal in Richmond to stop operations. The citizens risked arrest to protest mile-long oil trains that threaten the safety of area residents and are a massive new source of air and carbon pollution in the region.

- Five local residents have stopped work at a Burlington Northern Santa-Fe Rail Yard in Everett by erecting a tripod structure on the outbound railroad tracks, directly in front of both a mile-long oil train and a coal train.

- Energy giant BP’s willful misconduct and gross negligence led to the worst offshore oil spill in U.S. history, a federal judge said in a ruling Thursday that exposes the company to billions of dollars in civil penalties. The ruling from U.S. District Judge Carl Barbier could lead to nearly $18 billion in civil penalties for polluting the gulf. BP had already agreed to pay $4 billion in criminal fines. BP, which also owned the oil well, bears two-thirds of the blame for the spill, Barbier said, apportioning most of the rest to the rig owner, Transocean Ltd., and a small portion to the cement contractor, Halliburton.

- Energy Minister Andrew Younger announced Wednesday that the Liberal government plans to introduce legislation in the fall prohibiting hydraulic fracturing in shale oil and gas projects in the province.

- ThinkProgress.org reports that a new study predicts that a lack of available water could crimp energy development in many of the nations with the most abundant shale oil and shale gas resources.

Agribusiness

- Dozens of fast food workers have been arrested at protests around the country where they are demanding higher pay at popular restaurants such as McDonald’s, Burger King and Domino’s. Fast food workers in New York City, Chicago, Detroit and possibly more cities were arrested for blocking traffic in front of restaurants early Thursday morning, while thousands more continued protesting peacefully, according to news reports.

- A US Federal Appeals Court has ruled that biotech companies cannot force grain elevator companies to store GM produce. The case’s origin goes back to 2011 when Syngenta tried to force Bunge operators to hold a GM variety of corn. This ruling will set a precedence that can impact future similar cases brought to trial.

- A report was recently released from The African Centre for Biosafety (ACB) detailing the current domination of the agribusiness value chain in Africa by South African agribusinesses. The report discusses implications of South African agribusiness expansion and dominance in the continent, including blocking the emergence of small operators and producers, depressing local innovations, and negatively impacting food security.

- German supermarkets have demanded this week that the German Poulty Association (ZDG) stop using GM feed for egg and poultry meat production. The supermarkets want to receive GMO-free fed products by January 1, 2015, meaning that poultry producers are rushing to change their feed supplies. The demands from supermarkets come after investigating claims from the ZDG that there is not a sufficient supply of GMO-free soya. These claims have been found to be inaccurate and were retracted by the ZDG.

- The European Parliament (EP) held a debate on GMO cultivation and safety laws on September 3, 2014. This comes amid EU-wide discussions on changing legislation
regarding the status of GMO cultivation on the continent.

- On Tuesday, September 2, 2014, a class action lawsuit was filed on the Ontario Supreme court against Bayer and Syngenta. The case is being brought to the Ontario Supreme Court on behalf of all Canadian beekeepers, suing for damages resulting from widely used pesticides blamed for massive bee deaths. The lawsuit is being led by two of Ontario's largest honey producers, Sun Parlor Honey Ltd. and Munro Honey.

- The “Monsanto Law,” part of an agreement to protect strains of seeds developed by agribusiness corporations, has been suspended by Guatemala’s highest court. The writ was filed to suspend the law arguing that it would harm the nation. The ruling offers a period of 15 days for both major political parties in the country to offer arguments surrounding the case. Both parties have announced they will present arguments opposing the law.

- Russia is considering GMO sanctions on all food imports into the country. Experts including scientists and farmers have urged Russian PM Dmitry Medvedev to include GMO’s in existing food sanctions on the EU, US, and Australia. The ban would include all 18 varieties of GMO crops approved by Russia with the intention of causing the most economic stress to the EU and US. Monsanto is listed among the largest biotech companies that would be affected.

- Ethanol makers could export 1 billion gallons of ethanol, a sharp increase from 622 million gallons last year, if the government relaxes the requirement to blend biofuels into gasoline, said the head of an ethanol trade group.

- A Chinese woman charged as part of what federal prosecutors say was a conspiracy to steal trade secrets from U.S. seed corn companies is seeking to have her case separated from her brother's and wants a trial held as quickly as possible. In documents filed in federal court in Des Moines, the attorney for Mo Yun also asked a judge to force federal prosecutors to come up with more details about the charges. Mo, 42, was charged in July. She is one of seven people connected to Chinese agriculture biotechnology company DBN Group, which prosecutors say stole patented seed corn from fields in Iowa and Illinois and shipped it to China to try to reproduce its traits. The government says the value of stolen seed and the intellectual property of U.S. seed corn companies exceed $500 million.

- Corn advanced amid concern that an escalation of tensions between Ukraine and Russia may affect grain shipments from the Black Sea region.

- The UK's Farmers For Action is planning protests in the coming weeks after more milk processors announced heavy price cuts. As of Wednesday night (3 September), 820 farmers had voted for action on the group’s website.

Insurance/Healthcare

Insurance

- Federal officials have confirmed that hackers uploaded malware to a test server for the Obamacare insurance exchange website HealthCare.gov in July.

- Healthcare organizations have paid more than $10 million in HIPAA-related enforcement activities since June 2013, and, according to Jerome Meites, Department of Health and Human Services (HHS) chief regional civil rights counsel, more enforcement actions are coming.

- The quarterly Cloud Adoption and Risk (CAR) Report from Skyhigh Networks uses usage data collected from customers around the world to help explain how some enterprise organizations adopt and use cloud data. Though the High Tech industry led the way with an average of 193 data exfiltration events and 41 malware incidents per
quarter, healthcare was next on the list with 63 data exfiltration events and 29 malware incidents. Researchers made the point that, considering how regulated the healthcare and financial industries are, it's interesting that their risk activities are marginally higher than other non-regulated industries.

- Memorial Hermann Health System is notifying approximately 10,600 patients of an insider breach that spanned nearly seven years and involved improper access to electronic medical records.

- Insurance companies are well-versed in detecting and investigating fraud, often in partnership with law enforcement. Dealing with fraud once it occurs is expensive and time-consuming, so many state and local governments are stepping up efforts to stop fraud before it starts.

- HITRUST released the pertinent information and participant numbers for its CyberRX 2.0 program today, announcing that more than 750 healthcare organizations signed up for the cyber-attack simulation exercise that will begin in October.

- The umbrella vendor statement “we encrypt all of our data” isn’t enough to satisfy HIPAA regulations, nor is it sufficient for a healthcare organization to trust in those words as it’s building a strong security program.

- Duke University Health System recently announced that it experienced a patient data breach on July 1 when an unauthorized person stole an unencrypted thumb drive from an administrative building.

- Dashboard cameras are enjoying increased popularity by consumers concerned with protecting themselves from car insurance fraud.

- The price tag for resolving the data breach at Community Health Systems that affected 4.5 million patients could potentially exceed $100 million, by some estimates.

- Unlike the financial services industry, health care companies lack measures to adequately prevent identity theft, even as they continue to digitize medical records and other sensitive information.

- Huntington Bancshares Inc. Group Health Care Plan of Ohio notified HHS that 4,487 enrollees were affected by a hacking incident discovered on March 25th.

- Bulloch Pediatrics is warning patients that some of their personal information may have been compromised when a local storage facility was burgled. The practice stored some old insurance records and other payment records in those units.

- AltaMed Health Services is notifying affected individuals of a recent incident that may affect the security of their personal and protected health information. The organization learned from local law enforcement of an ongoing criminal investigation of a former AltaMed temporary employee, and other individuals unaffiliated with the organization, on suspicion of identity theft on June 30, 2014.

- Care All Management, LLC of Tennessee recently notified HHS of a breach that affected 28,300. The incident, described as “improper disposal,” was discovered on July 14, 2014.

- Six GTA hospitals compromised their patients’ personal health data by routinely handing it over to baby photographers who paid for access to maternity wards — breaches revealed by extra scrutiny following a major breach at Rouge Valley Health System. As far back as 2009, Mount Sinai, North York General, St. Joseph’s Health Centre, Humber River, Toronto East General and Rouge Valley Health System hospitals inappropriately gave up the information of tens of thousands of new mothers.
Financial

Activism

- Housing activists held an anti-eviction protest in Muskegon, MI on September 2nd in support of a local homeowner facing eviction by a leading U.S. bank.

- Activists held a Fair Wage rally at the Massachusetts State House in Boston, MA on September 4th in support of homecare workers.

- Activists staged an anti-foreclosure protest outside the Midwestern regional office of a GSE for housing in Chicago, IL on August 29th in support of a local homeowner facing foreclosure.

- Housing activists will hold a ‘Stop HUD Home Loan Sales’ protest outside the Chicago Regional Office of the U.S. Department of Housing and Urban Development (HUD) in Chicago, IL on September 9th.

- Housing activists will organize a ‘HUD National Day of Action’ event in Atlanta, GA on September 9th and deliver a petition to the HUD office in Atlanta asking the agency to reform the Distressed Asset Stabilization Program to keep families in their homes.

- Housing activists delivered a petition to a leading U.S. bank branch in Atlanta, GA, demanding that the bank meet directly with families affected by the bank’s “peddling of toxic mortgages and destruction of the U.S. economy.”

- Housing activists held a “housing tour” in Chicago, IL on September 7th in order to bring attention to the methods families are using to stay in their homes and occupy bank-owned properties. Anti-eviction groups in Chicago have previously organized similar bus tours and visited distressed borrowers, which has garnered media attention.

- Housing activists in Chicago, IL held an anti-eviction protest on September 6th in support of a local homeowner facing eviction by a reverse mortgage solutions company.

- A housing activist group will conduct a fundraiser event on September 12th in Minneapolis, MN with intent to raise funding for the group’s initiatives against banks and housing injustices. The event will include an “Ice Banker Challenge” in which participants will have the opportunity to soak a mock banker. The banker's “identity” will be revealed closer to the event date.

- Occupy Wall Street – affiliated housing activist groups will launch a Halloween-themed anti-bank action on October 31st at or near Hollywood Boulevard in Los Angeles, CA.

Information Security Risk

- Anecdotal evidence has emerged that the Russian botnet raiders behind the “biggest-ever” password theft have begun attacks against web services using stolen login credentials. The CyberVor gang is reported to have amassed a vast stockpile of compromised login credentials for “1.2 billion” accounts in August 2014 after breaking into 420,000 websites vulnerable to SQL injection attacks, among other techniques. An LA-based domain registrar and hosting firm warned on September 1st that hackers have begun using the list to try to access its users’ accounts. The vast majority of these login attempts have been unsuccessful as the data is incorrect or old, and passwords have been changed. As a precaution, the hosting company says they are aggressively blocking the IP addresses that appear to be logging in with the stolen password data.

- A security research firm discovered a watering hole attack that’s using a framework developed for reconnaissance as the primary infection vector. The criminals responsible for the incident compromised an unnamed industrial software firm’s website, suggesting
the potential for future attacks against several industries. The unnamed victim produces software used for simulation and system engineering for a wide range of industries including automotive, aerospace, and manufacturing. The attack starts on the compromised firm's website, where a malicious JavaScript file is loaded from a remote server. Unlike most watering hole incidents, where the visitor is infected with malware, this attack delivers a framework called Scanbox, which collects data from the victim and delivers it to the C&C (command-and-control) server. Using plug-ins, the framework has the ability to detect dozens of third-party software installations, including browsers, instant messengers, remote access software, business software, and security software. Finally, keylogging is used to capture data periodically, as well as when information is submitted by the victim to the compromised website.

- A new study said a staggering 15 million new malware samples were recorded during the second quarter of 2014, representing about 160,000 new samples being created every day during the period. Trojans, again topping the list of the most common types of malware, accounted for 58.2% of newly created risks. Potentially Unwanted Programs (PUPs) reported a substantial growth spurt (24.77%). The study noted that over recent months there has been a significant increase in the creation of software bundlers, programs that install PUPs on computers along with the programs that the user actually wants to install, without asking for the user's consent. Regionally, China (51%) was hit with the highest infection rate, followed by Peru (44.34%) and Turkey (44.12%).

- Researchers said the number of businesses hit by the data-stealing Backoff malware may be substantially more than the 1,000 or so companies estimated by federal officials. In the span of just a few days, the researchers discovered more than 100 systems from 85 distinct IP addresses attempting to connect to the two malicious command-and-control servers. Of that number, 69 of the infected systems were in the U.S and 28 were in Canada. The researchers also spied on communications from a smattering of infected systems in other countries, including the United Kingdom and Israel. Among those with infected systems were a global freight shipping and transportation company based in North America; a North American payroll association; a U.S.-based liquor store chain; and a U.S.-based Mexican food chain, the researchers said.

- Multiple banks said they were seeing evidence that a leading U.S. retailer of home improvement and construction products and services may be the source of a massive new batch of stolen credit and debit cards that went on sale last week in the cybercrime underground. A leading security researcher said new data gathered from the cybercrime underground suggests that the apparent payment card breach at the company involves nearly all of its stores across the nation. Other industry experts said there are signs that the perpetrators of this apparent breach may be the same group of Russian and Ukrainian hackers responsible for the data breaches at another US-based retailer, and an Asian-themed US casual dining restaurant chain, among others.

- Researchers said the number of US banks that have apparently been targeted and breached by hackers is slowly rising, as newer reports say that seven financial organizations have been hit. Industry experts also said the scope of the attacks is larger than initially thought, as one leading U.S. bank reported that the attackers changed and deleted some bank records.

- The Federal Bureau of Investigation said they did not find any evidence to suggest that the data breach incident involving the largest U.S. bank hit other banks in the country. However, people close to the investigation said the probe is continuing and could drag in other financial firms. The bank's own investigators have, however, found clues that a global network of computers available for hire by sophisticated criminals was used to reroute data stolen from the bank to a major Russian city. The investigators have identified what they believe to be the assault's staging ground, called a "bulletproof" hosting platform because of its resilience to other attackers and to law enforcement. The constellation of computers was used in previous hacking attacks and is now being tapped by professional cybercriminals operating out of Eastern Europe to target banks. Other sources familiar with the investigation said the cybercriminals operating the global network had also aimed at other banks' systems, though they may not have been hacked. The Financial Services Information Sharing and Analysis Center, which
monitors cyber threats on financial institutions, informed members on August 28 that there were no signs of a sophisticated and coordinated attack on banks, and the organization's threat level for the banks remains unchanged.

- A leading online security firm issued a security advisory on September 3rd, warning that attackers discovered a weakness in Linux systems they can exploit to expand their botnets and launch DDoS attacks. The favored target in this attack is the entertainment industry, though other business sectors are at risk as well. In this attack scenario, vulnerable Linux systems are infected with IptabLes and IptabLex malware. Attackers manage to compromise large numbers of Linux systems by exploiting vulnerabilities in Apache Struts, Tomcat and Elasticsearch. Attackers use the Linux vulnerabilities on unmaintained servers to gain access, escalate privileges to allow remote control of the machine, and then drop the malware into the system. This allows them to hijack those systems, which are then pulled into botnets used to launch DDoS attacks. Many industry experts call this a significant development because the Linux operating system is rarely used in DDoS botnets.

- A leading online security firm reported that an infamous banking malware known as Vawtrak is now equipped with more powerful weapons and is a much more substantial threat than it was a few months ago. The malware is the latest version the 64-bit compatible Gozi Prinimalka Trojan, a family of malware first conceived in the mid-2000's. The security firm said the malware's targets are growing outside the financial industry and geographic distribution continues to rise. Original Vawtrak attacks primarily targeted financial institutions in Japan, but recently observed configuration files extend attacks on social networks, online retailers, analytics firms, and game portals. Geographic distribution has also been expanded to specifically target: U.S., Canada, the UK, Australia, Turkey, and Slovakia.

- A San Diego, California-based hotel chain issued a notification that the payment card processing systems used at five of its San Diego locations were compromised and personal information, including credit card numbers, may be at risk. The company said that the potential number of affected customers is estimated to be between 40,000 and 45,000 and expiration dates may have been compromised, as well.

- A leading U.K. bank has teamed up with a Japanese technology company to produce a biometric banking authentication device which scans the vein patterns in customers' finger tips. The technology, a small box with an opening that attaches to the computer via USB, uses infra-red lights that scans the user's fingers and will allow them to access online accounts and make payments without the need for a PIN or password. The firms said that it is more secure than 'normal' finger scanning technology because the vein patterns and blood flow are very hard to replicate, with a one in a million chance of coming across two people who have very similar patterns. The U.S. bank said that the biometric reader will be rolled out in 2015.

- Researchers discovered a new Mac version of the XSLCmd backdoor that has been around since at least 2009. The Mac version shares a significant portion of code with the Windows version. The backdoor allows a remote attacker to launch a shell, do file listings and transfers, install executables and configure updates. But the Mac version has two new features: key logging and screen capture. The OS X version was submitted to VirusTotal on August 10th. No products found it then and, as of the scan at 2014-09-04 16:40:56 UTC, there were still no products that detect it.

Legal, Litigation, Regulatory Risk

- Financial reform advocates on September 4th renewed their push for regulations forcing corporations to disclose their political spending. The SEC signaled its intention to impose the requirements more than a year ago before shelving the plan amid fierce pressure from industry groups and congressional Republicans. Proponents of the regulation state that they gathered more than a million public comments from individuals and groups demanding that the SEC return the item to its formal rule-making agenda. They are pressing the SEC to re-list the proposal on its next regulatory agenda, due out some time this Fall.
Operational Risk

- A controversial upstart trading platform is nearing its goal to become a new stock exchange after raising $75 million in new funding that will be used to pursue registration as a U.S. national exchange. The alternative trading system is said to have been developed to compete against the larger banks and their high-frequency trading speed advantage. The platform claims to combat opaque high-frequency trading by slowing down orders to dampen the predatory effects of high-frequency traders.

- Investors will be able to trade A-shares listed in the Shanghai Stock Exchange via the Hong Kong Stock Exchange beginning in October 2014. This decision by the Chinese government came in support of a stimulus program in the Chinese economy. The move will allow the Chinese mainland companies to draw funds from a larger investor pool than they had access to previously. While investors may be excited to invest in the world’s second largest economy, industry experts note that investors may be wary of the corporate governance standards that are thought to be below Western standards. Furthermore, they might be put off by the dangers of investing in an unknown market, the access of which has so far been difficult, in addition to not knowing what to buy given the non-familiarity with the companies.

- An article published last week claimed that the Federal Housing Finance Agency’s proposal to change membership requirements in the 12 Federal Home Loan Banks will devastate housing finance far beyond its effect on real estate investment trusts. The proposed rule changes, announced September 2nd, would revise FHFA’s existing membership regulation to require that members maintain a commitment to housing finance and that only eligible entities can gain access to bank advances and the benefits of membership. Some industry experts claimed this is an anti-liquidity and anti-housing regulation, and a threat to the fundamental purpose of home loan banks.

Reputational Risk

- A housing activist group claimed that two GSEs for housing are taking too long to help troubled borrowers to reduce principal payments. According to the group, many loans were initiated during the crisis of 2007-2008 and many lenders have been forced into billions in settlement but those settlements have not offered much in the form of mortgage principal reductions.

- An op-ed published last week urged the U.S. government to sell the two GSEs for housing and not let them “sink or swim by themselves” because they are highly profitable and would be worth hundreds of billions in the open market.

- A housing activist group claimed to have investigated Atlanta, GA and 29 other metro areas and found evidence of discrimination in treatment of the properties that banks and GSEs owned. They found that banks and GSEs did not secure the doors and windows, mow lawns, fix gutters and downspouts, remove trash, or provide other maintenance in minority areas. After examining more than 2,400 foreclosed homes nationwide, including 65 in largely African-American neighborhoods in southwest Atlanta, the group concluded that those properties were about twice as likely to be poorly maintained as bank-owned houses in mostly white neighborhoods. The markers of neglect included overgrown and trash-strewn lots, and no evidence of “for sale” signs or other efforts to sell the vacant properties.

Global Intelligence

**Argentina**

- Federal police raided the headquarters of IT company Sonda in Buenos Aires, Argentina, as a result of a complaint filed by the Union Informatica labor union. The complaint alleges that physical attacks were carried out by Sonda managers towards a
union delegate who was trying to advocate for workers' rights during a strike.

- An Argentine media outlet reported that the minimum wage will increase by 23%, up to $4,400, in September, and by 8%, up to $4,716, in January. The measure was agreed by the Minimum Wage Council—formed by government, business, and union representatives. The new minimum will directly benefit registered workers earning the minimum wage—between 113,000 and 300,000 people—though it is also expected to affect the income of unregistered workers, for whom the minimum wage is used as a reference.

**Australia**

- On 9/4/2014 IT News reported that the Australian Crime Commission has suggested the Government consider penalties for internet service providers who fail to comply with requests from law enforcement to block websites.

**China**

- China’s Parliament rejected Hong Kong's demand for full democracy. The activists are calling their movement "Occupy Central". Pro-democracy groups pledged to unleash waves of protest to cripple Hong Kong’s financial centers. The Chinese Communist Party believes that there are forces in Hong Kong that want to undermine China.

- China Labour Bulletin reported that following a devastating explosion that killed at least 75 workers and injured 185 others last month in Kunshan, China’s national legislature will be increasing fines on companies involved in workplace accidents.

- The SAIC, China’s anti-monopoly regulator, asked Microsoft on Monday to explain issues related to the compatibility of its Windows operating system and Office software suite within 20 days. Microsoft stated on Monday that it will shut down the Windows Live Messenger (MSN) service in China on October 31 and migrate MSN users to Skype.

- Green America and China Labor Watch released an “Investigative Report of Catcher Technology Co. Ltd (Suqian), an Apple Parts Manufacturer” highlighting various labor and safety violations at the factory.

**Germany**

- On 9/1/2014 NPR reported that Amazon Germany workers are unhappy because they are classified as logistic workers an not retail workers. In Germany, retail workers are paid more than logistic workers. According to Verdi, the service workers union, Amazon fulfillment center wages start at 1,631 euros/month (about $2,150) and go up to 2,348 euros ($3,100).

**Israel**

- On 9/3/2014 the Globes reported that Histadrut leaders with SAP Israel employees, are negotiating for the founding of a workers committee to represent the employees, and hope to obtain the signatures of a third of the company’s 700 employees. If successful, the Ra’anana-based software company will have a representative workers committee for the first time.

**North America**

- On 9/4/2014 the WSJ reported that the judge in the antitrust case involving four tech companies set a 1/12/2015 trial date.

- On 9/5/2014 Mondaq reported that Philadelphia’s mayor signed City Council Bill 130992, amending Philadelphia’s Fair Practices Ordinance and making it illegal “for any employer to fail to reasonably accommodate an individual's need to express breast milk.”

- On 9/5/2014 Reuters reported that Silicon Valley tech companies in the anti-poaching lawsuit filed an appeal to Judge Koh’s decision to reject the proposed class action
On 9/4/2014 Democracy Now reported that activists have set 9/10/2014 as the day for "Battle for the Net's Internet Slowdown." Protesters will place their websites animated "loading" graphics (which organizer call "spinning wheel of death") to symbolize what the Internet might soon look like.

On 9/3/2014 JDSupra reported that the U.S. Court of Appeals for the Sixth Circuit has agreed to rehear the EEOC v. Ford Motor Co. The original decision, holding the Ford should have allowed an employee with severe and unpredictable irritable bowel syndrome to telecommute as a reasonable accommodation under the ADA, was issued by a 3-judge panel of the Sixth Circuit. The panel's decision has been vacated, and the appeal will be reheard en banc.

On 9/3/2014 Cult of Mac reported that Apple and Google have resumed mediation talks with tech workers who are suing Silicon Valley's top tech firms for an alleged anti-hiring agreement. Court filings indicate that Intel and Adobe are also participating in the talks as the companies attempt to reach a new settlement for the class action case after US District Judge Lucy Koh rejected companies' proposed settlement of $324.5 million last month. There were no commentaries in this article.

North Korea

North Korea's cyberwarfare capabilities are on the rise despite being entrenched in aging infrastructure and dampened by a lack of foreign technology. South Korea claims that North Korea's "premier" hacking unit, Unit 121, is behind the US and Russia as the "world's third largest cyber unit." South Korea estimated that North Korea's hacking team comprises of roughly 3000 staff, while a report released by South Korean publication Yonhap upgraded this figure to 5900. However, North Korea maintains heavy restriction on Internet use, which is censored by the state and only used by the social elite, meaning that any attacks originating from the country are highly likely to be state-sponsored, and rogue actors are unlikely to exist.

South Korea

A data breach in South Korea appears to have impacted as many as 27 million citizens, roughly 70 percent of the nation's population. The information contains individuals' names, resident registration numbers, account names and passwords.

Sweden

A recent study by KPMG, which spanned a four-week period reveals that during this time period 15, 586 security alerts were recorded. The study spanned 12 organizations covering different verticals and sectors. 93% of those participating organizations were breached during the given time, primarily through the existence of a call-back traffic, where malware had been planted on the host level to call a remote server and wait for a response. It suggested that advanced persistent threats were behind the threats sweeping Sweden.

Vietnam

On 8/30/2014 Viet Nam News reported that the Department of Network Security was official opened in Ha Noi on 8/28/2014 to keep an eye on Vietnam's internet traffic. Vietnam's Ministry of Information an Communication has issued a circular regulating the management of information on web portals and social network. According to the circular the Government will be able to identify social networks' users as the networks will be linked to the electronic database of the citizen's identification cards an the national system of personal social number. According to the circular, all the social network and web portals since 10/10/2013 must store at least two years of their information activities and the same time span for the information of the user's account, log-ins, log-outs and IP addresses on social networks. In addition, all contents on the web portals should be saved for at least 90 days since their posting time.
On 9/2/2014 Bubblew reported that Canon, Samsung, LG, and Microsoft/Nokia shifted their global production to Vietnam. The article stated that Wintek has also unveiled plans to Bac Giang Province that will double investment in Vietnam.

On 9/3/2014 Vietnam Briefing reported that results recently released by the U.S. Chamber of Commerce in Singapore shows that Vietnam is the 2nd most popular destination for U.S. business expansion among the member states of the Association of Southeast Asian Nations (ASEAN). Indonesia was ranked first.

**Legal and Regulations**

NIST is holding their 6th Cybersecurity Framework Workshop October 29-30, 2014 at the Florida Center for Cybersecurity (FC2) located at Univ. South Florida, Marshall Student Center, Oval Theater 4103 USF Cedar Circle, Tampa, FL 33620. Register [here](#) and view a draft agenda [here](#).

**New gTLDs**

As of August 22, 373 TLDs have been introduced to the internet, with 1,321 TLDs still proceeding

- The General Availability phase for [.global](#), [.london](#) & [.yokohama](#) will begin **September 9, 2014**.
- The General Availability phase for [.church](#), [.guide](#), [.life](#), [.loans](#) & [.versicherung](#), will begin **September 10, 2014**.

**Pharmaceuticals**

- ClearDATA Networks, Inc. announced that it has successfully achieved Common Security Framework (CSF) Certified status from the Health Information Trust Alliance (HITRUST). This independent, third-party certification assures healthcare organizations that ClearDATA’s cloud computing, backup, disaster-recovery and professional services meet the highest standards for managing security risks and protecting health information.

- A hacker broke into part of the HealthCare.gov insurance enrollment website in July and uploaded malicious software, according to federal officials. Investigators found no evidence that consumers' personal data were taken or viewed during the breach, federal officials said. The hacker appears only to have gained access to a server used to test code for HealthCare.gov, the officials said.

- Agora, another online black market is reported to have more product listings than other markets on the dark net after the FBI’s Silk Road bust in 2013. Agora’s biggest advantage is its large user base has attracted a critical mass of drug dealers, who in turn draw more customers.

- A massive medical device recall reported last week by the US Food and Drug Administration (FDA) is the largest-ever single-day event on record, according to data recently made available by FDA. The devices, which were manufactured by Puerto Rico-based device manufacturer Customed, Inc, were given a Class I recall classification—FDA’s most serious recall classification, given to those devices in cases where “there is a reasonable probability that the use of or exposure to a violative product will cause serious adverse health consequences or death.”

- U.S. officials on Thursday arrested a pharmacist linked to a 2012 outbreak of meningitis that killed 64 people across the United States as he was boarding a flight to Hong Kong, Justice Department officials said. Glenn Adam Chin, 46, had been a supervising
pharmacist at the now-defunct New England Compounding Center of Framingham, Massachusetts. It produced tainted steroids that sickened 700 people in 20 states in the worst outbreak of fungal meningitis recorded in the United States, officials said. Chin has been charged with mail fraud in connection with shipping 17,000 tainted vials, according to the U.S. Attorney’s Office in Boston. The contaminated vials were sent to more than 76 facilities in 23 states. The steroid, methylprednisolone acetate, typically was injected into patients to ease back pain.

- GlaxoSmithKline faces a shareholder revolt over plans to shake up its board, with leading investors calling for the speedy departure of chairman Sir Chris Gent. Several big institutions, riled by Glaxo’s poor share price performance and a growing catalogue of corruption claims, want a change this year.

- While the foreign-born make up just 13% of the U.S. population, they hold about 17% of the jobs in the U.S. pharmaceutical industry, according to a study by the Institute for Immigration Research at George Mason University in Fairfax, Va.

- Malware attacks are on the rise in many industries, but researchers from the security firm Websense say the rate at which attacks on hospitals has grown during the past year is unparalleled. Data security is often lax within health-care facilities, and hackers are targeting systems that store troves of valuable personal information held in electronic medical records, according to the Websense researchers, who say they’ve observed a 600 percent increase in attacks on hospitals over the past 10 months.

Retail

- A new report claims the apparent data breach at Home Depot could be “much, much bigger” than last year’s infamous Target infiltration. Evidence gathered by security blogger Brian Krebs suggests the breach involves nearly all of Home Depot’s 2,200-plus stores nationwide.

- Activist group, Rainforest Action Network (RAN), announced a new campaign called “Out of Fashion: a campaign for forest friendly fabric” which addresses the use of dissolved pulp in high-end clothing. The campaign coincides with Fall Fashion Week in New York City. A petition, which will be sent to fashion companies, has been posted on the RAN website.

- Family Dollar has rejected the revised proposal made by Dollar General on Sept. 2 on the basis of antitrust regulatory considerations.

- The Alibaba Group disclosed on Friday that it hoped to raise as much as $21.1 billion in its long-awaited initial public offering, setting up expectations for the biggest stock market debut in United States history.

Technology

- This week, some of the biggest tech companies will lead a symbolic “Internet Slowdown” to protest the Federal Communications Commission’s network neutrality proposal. “Several top websites—including Etsy, Kickstarter, Foursquare, WordPress, Vimeo, reddit, Mozilla, Imgur, Meetup, Cheezburger, Namecheap, BitTorrent, Gandi.net, StartPage, BoingBoing, and Dwolla—announced that they will be joining more than 35 advocacy organizations and hundreds of thousands of activists in a day of action that will give a glimpse into what the Internet might look like if the FCC’s proposed rules go into effect,” the advocacy group “Fight for the Future” said.

- China’s State Administration for Industry and Commerce (SAIC) has questioned Microsoft Vice President Chen Shi regarding allegations of abuse of Microsoft’s
monopoly on operating systems, software products, and browsers in the country. Microsoft has been given 20 days to respond to complaints alleging that Microsoft’s use of serialization of software may have violated China’s anti-monopoly laws.

- Europol has launched a cooperative cybercrime busting outfit called J-Cat, or the Joint Cybercrime Action Taskforce. The taskforce is made up of representatives from forces of member states in Austria, Canada, the US, the UK, Germany, France, the Netherlands and Spain. Australia and Colombia are also expected to join. It has the backing of the European Union (EU) Cybercrime Taskforce, the US Federal Bureau of Investigation (FBI) and the UK National Crime Agency.

- Hackers build a Skype to subvert NSA’s mass surveillance program. Project, “Tox” is available for download and to use. The Tox team is trying to do, besides provide encryption, is create a tool that requires no central servers whatsoever—not even ones that you would host yourself. It relies on the same technology that BitTorrent uses to provide direct connections between users, so there’s no central hub to snoop on or take down.

- Less than a week ahead of the likely launch of Apple’s next-generation iPhones, the company is once again facing scrutiny over its labor sourcing in China.

- The White House confirmed that Megan Smith, vice president of Google’s super-secret Google[X] research lab, will be the new Chief Technology Officer of the United States.

- On 9/4/2014 Threat Post reported that cable modems sold by two manufacturers expose a wide variety of sensitive information over SNMP, including usernames and passwords, WEP keys and SSIDs. The broadband modems, manufactured by Netmaster and ARRIS, leak the sensitive information through the exposure of the SNMP community string. That string is a kind of password that is sent in cleartext by clients as a form of authentication.

### Telecommunications

- Rogue cellphone towers have been discovered in the USA. The fake cellphone towers were used by unknown threat actor(s) to eavesdrop mobile communication.

### Entertainment

- In what is often referred to as the celerity photo hack, iCloud accounts of female actors and athletes were targeted in a hacking attack and compromising private images of were posted online. It seems that the attackers might have either simply guessed passwords or used brute force attacks to gain access to victim’s personal files. However, Apple denies that a breach within the iCloud environment or an exploitation of the Find my iPhone feature were relevant in the cases investigated. Instead, the company suggested in a statement that weak passwords and security questions might have contributed to the widely published incident. However, Apple has announced to implement enhanced security measures by adding alerts and emails to caution users of potential account theft.

### Defense
A group of hackers known for past cyberespionage attacks against the U.S. Defense Industrial Base, as well as companies from the electronics and engineering sectors, has recently started using a backdoor program to target Mac OS X systems.

The United States military intends to deploy multi-purpose sensors in Canada’s Arctic that would sniff out a wider range of potential threats than just intercontinental ballistic missiles. These state-of-the-art systems would be designed to track maritime vessels, airplanes and small cruise missiles, all in addition to any large missile fired off by North Korea or some hypothetical rogue state.

The United States government has started a new campaign to fight global terrorism against the Islamic State and Al-Qaeda on social media.

Ministers are due to ratify NATO’s new cyber defense policy. The new policy means that a digital attack can now be considered as the equivalent of an attack with tanks or rockets and could trigger NATO’s collective defense clause.

The four armed services only submitted their draft 2016 budgets to the Office of the Secretary of Defense recently, and Undersecretary Frank Kendall said he’s already “concerned.” As the Pentagon’s top weapons buyer, Kendall sees worrying signs. With the automatic budget cuts known as sequestration looming in 2016, he said, officials are often low-balling cost estimates to preserve their current programs while shorting long-term investments in future weapons.

Iran’s air defense commander, Brigadier General Farzad Esmaili, claimed in a series of announcements made on 28 August and 1 September that the Islamic Republic is making progress on two indigenous long-range surface-to-air missile (SAM) programmes.

Boeing raised its forecast for jetliner demand in China, which is expected to eclipse the U.S. as the single largest airplane market by 2030.

France threatened to halt the controversial delivery of a warship to Russia, arguing that the Kremlin’s support of breakaway forces in eastern Ukraine endangered Europe.

**Law Enforcement**

- The Justice Department launched a broad investigation into the police department in Ferguson, Missouri, following recent unrest. The investigation, which is separate from an existing federal probe into the Aug. 9 shooting of Michel Brown, will look for patterns of discrimination within the predominantly white department and focus on how officers use force, search and arrest suspects, and treat inmates at the city jail. The police department said it welcomed the investigation.

- A superior court judge in Los Angeles County has sided with the Los Angeles Police Department and the Los Angeles County Sheriff’s Department in ruling that License Plate Reader (LPR) data is not subject to disclosure. The release of the data had been sought by the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF). A key part of the ruling was that the records were exempt under the California Government Code that allows records of an investigative nature to be withheld.