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 / Healthcare
- Financial Services
- Global Intelligence
- Legal and Regulations

New Webcast: Concrete Steps to Deploy an Effective Threat Intelligence Capability

Protecting your business — including its information and intellectual property, physical infrastructure, employees, and reputation — has become increasingly difficult. Among thought leaders and advanced organizations, the consensus is now clear. To adequately protect company assets and ensure business continuity, organizations must be more proactive and make effective use of threat intelligence.

Click Here To Learn More

Top Incidents
Energy

- An ongoing cyber-espionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers, known to Symantec as Dragonfly, managed to compromise a number of strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to energy supplies in affected countries. Among the targets of Dragonfly were energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland.

Agribusiness

- UK Farmers and meat processors agreed to draw up a voluntary code of conduct for the beef industry at a government-led summit. Representatives from the farming unions and the British Meat Processors Association (BMPA) will meet over the summer to discuss a code to increase transparency.

Insurance/Healthcare

- The Association for the Advancement of Medical Instrumentation (AAMI) and ECRI Institute recently released a report aimed at medical device and healthcare delivery executives to review technology safety trends. The report, titled Executive Insights on Healthcare Technology Safety, analyzed these safety concerns in the healthcare industry: alarm systems, Luer connectors, cybersecurity, batteries, and recalls. In looking at the cybersecurity portion, it's clear that many healthcare organizations are still suffering from major security configuration and testing issues.

Financial Services

- Researchers said a new Brazilian scam using “boleto,” (officially “Boleto Bancario”), a popular online payment method in Brazil that is used by consumers and for most business-to-business payments, is on the rise. The scam is typically done through malware that lies in wait until the user of the hacked PC visits their bank’s site and fills out the account information for the recipient of a boleto transaction. In this scenario, the unwitting victim submits the transfer for payment and the malware modifies the request by substituting a recipient account that the attackers control. It is estimated that a fraud ring known as the “Bolware” gang affects more than 30 different banks in Brazil and may be responsible for up to $3.75 billion USD in losses. Most Brazilian banks require online banking customers to install a security plug-in that hooks into the user’s browser. The plug-ins are designed to help block malware attacks. But according to researchers, the Bolware gang’s malware successfully disables those security plug-ins, leaving customers with a false sense of security when banking online. The malware also harvests usernames and passwords from victim’s PCs, credentials that are thought to be leveraged in spreading the malware via spam to the victim’s contacts. RSA said this fraud gang appears to have infected more than 192,000 PCs, and stolen at least 83,000 sets of user credentials.

Global Intelligence

- A Costa Rica media outlet reported that StarTek, a U.S. provider of business outsourcing services, will close its call center in Costa Rica on Aug. 30. The closure would mean the dismissal of the company’s 550 employees at their America Free Zone facilities in the province of Heredia, who managed customer relations and technical support calls, primarily for U.S. telecom companies. The media also noted that the StarTek president and CEO Chad Carlson said that the decision to close the facility was part of their strategic plan to optimize capacity. The closing adds to those by Intel’s manufacturing center, Bank of America financial services center, PET Packaging, and appliance
Legal and Regulations

- As of July 1, 2014, the U.S. government will start imposing a 30 percent tax on many overseas payments to financial institutions that don’t share information with the IRS as part of the Foreign Account Tax Compliance Act of 2010.

Energy

- An ongoing cyber-espionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers, known to Symantec as Dragonfly, managed to compromise a number of strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to energy supplies in affected countries. Among the targets of Dragonfly were energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland.

- Business Week reports that making the electricity grid greener is boosting its vulnerability to computer hacking, increasing the risk that spies or criminals can cause blackouts. Adding wind farms, solar panels and smart meters to the power distribution system opens additional portals through which hackers can attack the grid, according to computer security experts advising governments and utilities. The communication networks and software that link green energy sources to the grid as well as the electronic meters that send real time power usage to consumers and utilities are providing new back-door entry paths for computer hackers to raise havoc with the grid.

- This week (July 6-14) is the North American Week of Action to Stop Oil by Rail. Multiple environmental groups are staging protest actions in the United States and Canada throughout the week.

- The Sierra Club is organizing to oppose fracked-gas exports from the United States.

- A recent report questions BNSF’s safety record. This is being used to inspire opposition to oil train shipments.

- The activist website blue skies announces three opportunities to stop coal exports this summer. The opportunities include a demonstration by the tracks used to transport coal through Missoula the weekend of July 19th.

- Greenpeace activists protest on July 1, 2014 at Ambre Energy’s downtown Portland office against a plan to provide $2 million in public funds to help the financially shaky Australian company’s coal export proposals.

- According to a release from the UMWA, the union plans to host a rally in Pittsburgh on July 31. The union says the EPA’s existing power plant rule will cost tens of thousands of jobs for UMWA.

- German Greens Party members staged a demonstration in front of German Chancellor Angela Merkel’s office in Berlin in a protest against intensive use of coal in energy generation.

- A federal judge has blocked a coal mine expansion planned in Gunnison County, ruling that federal authorities wrongly ignored carbon costs when approving the expansion of Arch Coal Inc.’s West Elk Mine.
Thirty-five Greenpeace activists took part in a protest against EU energy policies at an EU summit in Brussels on 6/27. Early on Friday morning, amid tight security, activists unfurled giant banners blaming Europe’s largest energy companies for fuelling the EU’s dependence on energy imports. The climbers from six European countries – Germany, Belgium, the UK, France, the Netherlands and Switzerland – voluntarily gave themselves up to police. It is as yet unclear what charges they will face.

Police spied on protesters at Britain’s biggest anti-fracking demonstration, using bugging devices and infiltrating them with undercover ‘covert human intelligence sources’, an official report has revealed. The incendiary revelation emerged only because blundering police failed to properly redact the highly sensitive report.

The Moms Clean Air Force has started a petition urging the EPA to limit methane pollution from the natural gas industry.

CBS news discusses the finding of an analysis conducted by a Cornell University-led research team and published this week in the Proceedings of the National Academy of Sciences. The study finds that a large percentage of oil and gas wells tapping the Marcellus Shale region of Pennsylvania are leaking methane gas, either into the air or into underground sources of drinking water. It determined that unconventional gas wells in northeastern Pennsylvania had a nearly three-fold higher risk of leaking, compared to conventional wells in the same region. One possible factor for this so-called "methane migration," according to the study, could be "compromised structural integrity" in the casings and cement used in the unconventional oil and gas wells.

Vincent Sheheen, a Senator and candidate for governor of South Carolina, has started a petition calling on the Savannah River Site facility not to accept nuclear waste from Germany.

News report that New York’s highest court has upheld the bans on natural gas drilling passed by two small Upstate towns.

Agribusiness

- Organizers submitted petitions signed by 150,000 Oregonians, nearly double the number needed, to put a referendum on the November ballot to label food made with genetically modified organisms.

- A Chinese woman has been arrested and charged with trying to steal patented U.S. seed technology as part of a plot to smuggle types of specialized corn from farm fields in the U.S. Midwest for use in China, authorities said Wednesday.

- The woman, Mo Yun, is married to the founder and chairman of a Chinese conglomerate that runs a corn seed subsidiary. She and her brother, Mo Hailong, who also goes by the name Robert Mo, worked together and with several others from China to steal the valuable corn seed from Iowa and Illinois, according to law enforcement officials.

- UK Farmers and meat processors agreed to draw up a voluntary code of conduct for the beef industry at a government-led summit. Representatives from the farming unions and the British Meat Processors Association (BMPA) will meet over the summer to discuss a code to increase transparency.

- Both sides of a West Coast labor dispute are entering extra time as the contract between the Pacific Maritime Association and the International Long Shore and Warehouse Union officially expired June 30. As expected, both sides are negotiating in an effort to avoid the economic damage from a costly strike on the docks that, according to a recent study, could cost as much as $2.5 billion per day.
• On July 1, 2014, Sustainable Pulse reports that Monsanto and Pioneer have been quietly pulling applications to grow GM crops in the EU. It is reported to be revealed in the minutes of a meeting of the "Standing Committee on genetically modified food and feed" (SCFCAH) that Monsanto has retracted applications for two glyphosate-tolerant seeds, soybean 40-3-2 and maize line NK603. Pioneer has also withdrawn two applications of GE maize, lines 1507 x NK603 and 59122 x 1507 x NK603.

• In a study published last week taking surveys of over 1,200 households across the US, researchers found that avoiding GMOs was listed as the top reason for buying organic foods. 25% of parents already buying organic foods listed this response, which grew from 13% in 2013. The study also found that 73% of parents knew what GMOs were, indicating increased awareness of organic topics.

• Home Depot and other companies have announced that they will limit their use of neonicotinoid pesticides, suspected of "helping cause dramatic declines of honeybee populations..." Home Depot will be requiring labeling of plants using such pesticides by the fourth quarter of this year. The story has been posted by Facebook groups including one post included in the supplemental section of this report.

Insurance

• The College of Healthcare Information Management Executives (CHIME) and the Institute for Health Technology Transformation (iHT2) have joined to host a series of regional one-day educational programs this fall. These programs, called the Leadership Education and Development (LEAD) Forums, will aim to provide outreach and educational support to healthcare CIOs and other information security executives.

• Pet insurance fraud is thought to cost the industry £2m, according to figures released for 2011 by the Association of British Insurers, a vast hike from the previous year when it was estimated at only £420,000.

• The San Antonio Metropolitan Health District recently alerted families of just fewer than 300 child patients that their vaccination records had been breached after a city-owned laptop was stolen.

• A federally backed consortium of behavioral health providers, administrators and health information exchange experts has joined the chorus of voices addressing the vexing issue of how to pass along medical records for behavioral health patients without violating their privacy rights.

• The Alabama Department of Public Health (ADPH) has notified more than 500 patients who were treated at one of Alabama’s 65 county health departments that their personal information and identities were compromised.

• The Association for the Advancement of Medical Instrumentation (AAMI) and ECRI Institute recently released a report aimed at medical device and healthcare delivery executives to review technology safety trends. The report, titled Executive Insights on Healthcare Technology Safety, analyzed these safety concerns in the healthcare industry: alarm systems, Luer connectors, cybersecurity, batteries, and recalls. In looking at the cybersecurity portion, it’s clear that many healthcare organizations are still suffering from major security configuration and testing issues.

• The U.S. Department of Health & Human Services has launched a federal probe into HIPAA privacy violations at the University of Cincinnati Medical Center. The investigation stems from when a financial services employee of the hospital accessed the detailed billing records of a patient with a sexually transmitted disease and shared them with someone who deliberately and maliciously published those records on Facebook,
taunting and ridiculing the patient.

- A lawsuit filed in an ongoing dispute between a Connecticut community health center and its former IT director over an alleged security breach reveals more details about the issues involved. The lawsuit is another component of an acrimonious dispute, which also involves an investigation by Connecticut’s attorney general into an alleged security breach potentially affecting data of up to 130,000 patients.

- On 6/30/2014 Planet Princeton reported that Princeton HealthCare System will pay $1.35 million and will undertake significant remedial measure to settle a disability discrimination lawsuit brought by the US EEOC. The EEOC’s suite alleged that the hospital's fixed leave policy failed to consider leave as a reasonable accommodation, in violation of the Americans with Disabilities Act. According to EEOC, Princeton HealthCare’s leave policy only merely tracked the requirements of the federal FMLA and employee leaves were limited to a maximum of 12 weeks. The policy meant that employees who were not eligible for leave were fired after being absent for a short time, and many more were fired once they were out more than 12 weeks.

---

**Financial Activism**

- Housing activists leading an anti-eviction campaign in Chicago, IL are planning a phone campaign against a local property management company that lost one of its apartment buildings to foreclosure by a leading U.S. bank. Tenants at the building are negotiating with the lender to stop the impending lockout.

- Housing activists will march to demand affordable housing in New York City on August 21st.

- Environmental activists entered two leading U.S. bank branches in Washington, D.C. on June 28th to protest and demand the bank sever their ties to a builder of the Keystone XL tar sands pipeline. Within the first branch, protesters were able to reach the bank’s counter and attempted without success to hold a discussion with the bank manager. Afterwards, activists rolled out yellow “caution” tape outside the bank, and passed out flyers to passers-by. Activists then traveled to a second branch where they were able to access the ATM vestibule between the inner and outer doors before a bank employee locked the inner doors.

- Activists against the apartheid wall in the West Bank, Israel will conduct a 'National Week of Action' from July 6th to 13th across the U.S., calling on leading investment banks to divest from companies profiting from the Israeli occupation of Palestine.

- Occupy Wall Street conducted its 'Occupy the Vote 2014' kickoff event on July 1st at NYC City Hall to advocate taking back grassroots power of the people through their right to vote.

- Numerous activist groups will unite for a National Day of Action against the EU-US trade deal (TTIP) on July 12th at various locations throughout Europe, including Central London. Activists claim the TTIP is “threatening to be the biggest corporate power grab in a decade.” Participants are encouraged to “take to the streets” with likely protest actions.

- “Hundreds” of city workers and their allies packed the streets and sidewalks outside Los Angeles City Hall on July 1st protesting “predatory fees” the city pays to Wall Street banks. A coalition which includes labor unions, clergy and community groups, argued that the city must renegotiate two deals signed with banks in order to restore funding for
tree trimming, sidewalk repairs and other badly needed services. After a morning rally outside a downtown bank, dozens of city trash trucks slowly circled City Hall, blaring their horns, as workers clanked cowbells and chanted, “Fix LA!”

- A public post authored by Occupy Wall Street discusses financial firms’ alleged continued corruption and lack of regulation, while vowing continued attacks upon financial institutions starting with a leading U.S. investment bank headquartered in New York City.
- Housing activists in Minnesota hosted a training event on July 1st in Minneapolis in which members taught participants direct action tactics.

**Information Security Risk**

- Researchers detected a new banking malware called ‘EMOTET,’ which is capable of “sniffing” network activity to steal information. Once installed on the victim’s computer, the malware starts capturing and logging all outgoing network traffic. The most notable feature of this malicious tool is that it has the capability to extract data sent over a secure connection because it can hook into multiple network components.

- The Center for Internet Security (CIS) has revealed a study that suggests that APT hackers successfully compromised the networks of two US airport networks in the summer of 2013 as part of a major campaign targeting dozens of others.

- The Office of the Comptroller of the Currency has once again singled out cyber threats as a leading operational risk for U.S. banking institutions. The OCC noted in its report, Semiannual Risk Perspective for 2014, that banking institutions continue to be among the preferred targets for cyber-attacks, and that recent attacks against the retail industry have only reinforced why banking institutions need to be diligent about cybersecurity.

- Researchers have been observing proliferating malware infecting South Korean Android users at a rapid rate. The malware pretends to be a popular game or tool on third party Android markets and fools the user into downloading it. Once installed, it replaces their banking apps with fake versions that are designed to steal personal information including user IDs and passwords for online banking accounts.

- An investment brokerage firm based in St. Louis, MO suffered a data breach in May by an unauthorized third party in which client and employee information was compromised.

- According to a recent survey, 41% of global organizations suffered a DDoS attack over the past year, with more than 78% targeted twice or more. According to the BT-commissioned research, which covered 11 countries, DDoS attacks are seen as a key concern by a third of UK organizations (36 percent), although they seem to worry less than their international rivals: globally, almost twice as many organizations (58 percent) named DDoS as a key concern.

- Researchers identified a spear-phishing campaign using an Office Macro attack vector that targets victims in banking, oil, television, and jewelry industries. Cybercriminals take advantage of the Visual Basic Scripting for Applications feature in Microsoft Word to deliver the malware to the victim’s computer. When the victim opens the Word document, an On-Open macro fires, which results in downloading an executable and launching it on the victim’s machine. Using macros in malicious campaigns is an old approach, but in this case, the threat actors have combined the cloud storage services from Dropbox to host the payloads. Luring the victim to open the document is done through an email that purports to be an invoice, purchase order or receipt created specifically for the target. Should the victim launch the attached Word file, the malicious executable is retrieved from Dropbox by the macro and once on the computer, it contacts several domains.

- A leading food-service POS and security systems provider announced that a remote-
access attack on their systems may have resulted in the exposure of payment card transactions conducted at several national restaurant chains throughout the northwestern U.S.

- A hacker group claimed to have taken down the website of a leading Ukrainian bank owned by one of the nation’s oligarchs, Igor Kolomoisky, who is also one of the sponsors of the so-called National Guard waging a war on the country’s self-defense fighters and civilians in southeastern Ukraine.

- Hackers claimed to have decrypted over 438k credit and debit card accounts from the Ukrainian bank owned by Igor Kolomoisky and threatened to start “depleting all accounts” on July 5th if their terms for peace in Eastern Ukraine are not met.

- Researchers identified a new variant of the infamous ZeuS Trojan, dubbed Zeus Lite, which relies only on TCP to communicate to the remote server and has the initial server list encrypted and hardcoded in the malware body, together with the packet cipher key. The malware’s communications are encrypted with an AES-128 algorithm, and it can perform commands for shutting down the system, rebooting it, executing external programs or scripts, or updating the malicious components.

- Researchers said a knockoff of the Cridex banking Trojan has surfaced with new capabilities that can do more than steal online banking credentials. Dubbed Geodo, the malware comes with an efficient self-replicating feature borne of stolen SMTP credentials from compromised computers in the Cridex botnet. Geodo is a classic data-exfiltration Trojan that swipes everything from system information, to email credentials, banking log-ins and much more. Confined mostly to Western European targets—Germans in particular—Geodo has a striking new feature where it can turn any bot under the hackers’ control into a vehicle for infecting new targets. Once a bot is compromised by Geodo, the malware downloads an email worm that opens a backdoor channel to a command and control server which sends the bot a list of 50,000 stolen SMTP account credentials which are spammed out 20 at a time. Once the credentials have been sent, the emails are composed with a chosen sender address, subject line and body unique to a particular campaign. Every hour, a new batch of 20 emails is sent, in addition to new sender addresses, subject lines and body text, and the cycle starts over again. Geodo (past variants were also known as Bugat) is targeting victims from Germany, Austria, Hungary and the United States, primarily.

- A hacker group claimed to have taken down the website of a leading Israeli bank.

- Researchers said a new Brazilian scam using “boleto,” (officially “Boleto Bancario”), a popular online payment method in Brazil that is used by consumers and for most business-to-business payments, is on the rise. The scam is typically done through malware that lies in wait until the user of the hacked PC visits their bank’s site and fills out the account information for the recipient of a boleto transaction. In this scenario, the unwitting victim submits the transfer for payment and the malware modifies the request by substituting a recipient account that the attackers control. It is estimated that a fraud ring known as the “Bolware” gang affects more than 30 different banks in Brazil and may be responsible for up to $3.75 billion USD in losses. Most Brazilian banks require online banking customers to install a security plug-in that hooks into the user’s browser. The plug-ins are designed to help block malware attacks. But according to researchers, the Bolware gang’s malware successfully disables those security plug-ins, leaving customers with a false sense of security when banking online. The malware also harvests usernames and passwords from victim’s PCs, credentials that are thought to be leveraged in spreading the malware via spam to the victim’s contacts. RSA said this fraud gang appears to have infected more than 192,000 PCs, and stolen at least 83,000 sets of user credentials.

**Legal, Litigation, Regulatory Risk**

- An article published last week reported that Wall Street is mobilizing to defend its latest
tactic to keep overseas derivatives beyond the reach of U.S. rules. The industry’s main lobbying group is prepping a strategy to explain why the new practice -- removing guarantees from U.S. banks’ overseas trading -- is a lawful response to the 2010 Dodd-Frank Act and not an effort to take advantage of a loophole.

- An article published last week reported that the House Financial Services Committee's Subcommittee on Capital Markets and Government Sponsored Enterprises conducted a hearing on June 27th titled “Oversight of the SEC's Division of Trading and Markets.” Chaired by Rep. Scott Garrett (R-N.J.), Garrett identified two major areas where he would like to see change at the SEC — a thorough analysis of the markets in order to achieve a level playing field and Regulation National Market System, presumably to be measured against the SEC’s mission to maintain fair, orderly, liquid markets.

- A local family in the Seattle, WA area sued a leading U.S. bank for selling their home at auction without proper notification.

**Operational Risk**

- An article published last week reported that the Office of the Inspector General (OIG) for the Federal Housing Finance Agency (FHFA) released a report highlighting the risks with banks that serviced mortgages backed by the nation's two Government Sponsored Enterprises for housing, selling the rights to service troubled mortgages to nonbank servicers that specialize in handling them. The post indicates nonbanks hold approximately $1.4 trillion in mortgage servicing out of the nearly $10 trillion market, and these new servicers have less stringent regulatory and financial requirements than traditional banks.

**Reputational Risk**

- An article published last week on a free online stock message board site claimed that more than one third of equity trading in the United States and Europe is done outside the public exchanges, and most major banks run dark pools. The article also said banks also control the other 2/3rds of equity trading with their Specialist or now "designated market makers," market makers, trading platforms, option houses, commodity exchanges, etc. And they operate them as they please because they own the Federal Reserve, the SEC, the CFTC and the majority of our Politicians.

**Global Intelligence**

**Costa Rica**

- A Costa Rica media outlet reported that StarTek, a U.S. provider of business outsourcing services, will close its call center in Costa Rica on Aug. 30. The closure would mean the dismissal of the company’s 550 employees at their America Free Zone facilities in the province of Heredia, who managed customer relations and technical support calls, primarily for U.S. telecom companies. The media also noted that the StarTek president and CEO Chad Carlson said that the decision to close the facility was part of their strategic plan to optimize capacity. The closing adds to those by Intel's manufacturing center, Bank of America financial services center, PET Packaging, and appliance manufacturer and distributor MABE.

**Europe**

- On 6/30/2014 WRAL TechWire reported that the European Union has given approval to Lenovo's acquisition of Google Motorola Mobility. Lenovo is still awaiting words from US regulators.
Some British media (The Guardian, BBC, and Daily Mail) received notifications from Google that certain articles won't show up in search results any longer. EU citizens have the right to demand the removal of links from search engine results, if the individual's privacy rights trump the interest of the public to have the information available. The Right to Be Forgotten is a dimension of privacy protection established by the European Court of Justice. This does not necessarily mean that the information is removed at the source itself (e.g. an article on the newspaper’s website). Google apparently received over 70,000 removal requests so far.

India

- On 7/2/2014 The Hindu reported that Cisco announced that it has signed a pact with the Electronics City Industrial Association to develop Asia's first Internet of Things hub in Bangalore, India.

Mexico

- IndustriALL Global Union reported that the company CB&I Matamoros which manufactures stainless and carbon steel pipes in a range of alloys and other metallic structures is carrying out mass dismissals in Mexico after 350 workers went on strike demanding better working conditions and for freedom of association. The workers' main demand is for the company to comply with ILO Convention 87 and respect their decision to join IndustriALL Global Union affiliates Mexican Miners' and Metalworkers’ Union (SNTMMSRM). However CB&I has refused to respect freedom of association and has imposed the Day Laborers and Industrial Workers’ Union of the Maquiladora Industry (Sindicato de Jornaleros y Obreros Industriales y de la Industria Maquiladora de H. Matamoros), affiliated to the CTM.

North America

- On 7/7/2014 the Tammp Tribune reported that a group of Democratic lawmakers recently sent a letter to the FCC demanding it do everything in its power to let cities build competitive fiber networks.

- On 6/30/2014 the Seattle Times reported that 14 the U.S. Supreme Court ruled that thousands of Illinois home-health-care workers cannot be forced to pay fees to the SEIU to cover collective-bargaining expenses. This decision will affect union's ability to collect mandatory dues from workers. The court’s 5-4 decision said such mandatory fees violate the free-speech rights of workers who disagree with union political activities.

- On 6/30/2014 Venture Beat reported that President Obama made an official announcement that he will not pressure Congress to pass a bill for immigration reform this year and is, instead, unilaterally taking a few actions on border security. According to the article, this mean that there will be no major changes in the number of high-skilled immigrant visas to relieve the technology's tech-talent shortage.

- On 7/1/2014 CNet reported that Amazon is suing a former Amazon Web Services manager who left the cloud computing unit to work for Google's competing service. Amazon alleged that its former employee violated a non-compete agreement he signed when he first started working for Amazon.

- On 6/28/2014 Mobile Phone Adviser reported Microsoft's takeover over of Nokia's gadget and services department has been approved by both the US Department of Justice and the European Union.

- Broadcast television alternative Aereo has asked its supporters to join a “Protect My Antenna Protest” in a fight against the Supreme Court’s recent ruling against the company. Although it is commonly assumed that the ruling against the use of Aereo will mark the end of the service, it is now influencing supporters to ask Congress for the passing of a law that could give the company a second chance.
On 7/7/2014 the Tampa Tribune reported that a group of Democratic lawmakers recently sent a letter to the FCC demanding it do everything in its power to let cities build competitive fiber networks.

On 7/2/2014 RRStar.com reported that the US EEOC is suing Wal-Mart Stores over the firing of an intellectually disabled employee whose performance faltered when bosses no longer gave him written list of job tasks to do. The EEOC alleged that the written list of job tasks was the accommodation for the plaintiff's intellectual disability and that Wal-Mart failed to provide such accommodation causing plaintiff to fail in his duties and lose his job.

Russia

On 6/30/2014 Telecompaper reported that Russian cable TV industry group AKTR has issued a statement protesting against the draft law to introduce a ban on advertising over pay-TV services. The amendment to the Law on Advertising has been presented to the lower chamber of Russian parliament. According to the statement, the draft law wasn’t discussed with professionals from the pay-TV sector. The industry group claims that the advertising ban will force pay-TV operators to raise rates for services.

Korea

On 6/30/2014 InAutoNews reported that South Korea's biggest automaker could have its workers enter strikes, warns their union leaders, as the company and its labor representatives have reached a stalemate in their ongoing negotiations. According to the union, the demands for this year include a 7% or 159,614 won ($157) monthly wage hike, bonuses worth 30% of Hyundai's net income and to set the work hours per week limit at 52.

On 6/29/2014 the Korea Herald reported a union of contract workers for Samsung Electronics Services, most of whom are hired via Samsung's partner companies, agreed with the firms to settle a string of labor issues, such as the adoption of a monthly salary instead of piecework and supportive measures for union activities.

Vietnam

On 7/3/2014 Vietnam+ reported that Ho Chi Minh City is in need of some 150,000 workers in the remaining months of this year, notably skilled ones.

On 6/29/2014 Yahoo!News reported that Vietnam's GDP expanded 5.18% in January-June from the same period last year according to General Statistic Office estimates, up from 4.9% in the same period last year.

On 7/2/2014 Yahoo!News reported that Samsung Display Co Ltd, a subsidiary of Samsung, announced that it received approval to build a $1 billion display module assembly plant in Vietnam, its first production facility in the country. The plant will be built in Bac Ninh province in Vietnam and production is scheduled to start in 2015.

On 6/29/2014 Vietnam.Net, a local VNese media source, reported that Microsoft, the Viet Son Company, and Intel Corporation officially launched the first VNese brand tablet in Vietnam market, namely ROSA.

Legal and Regulations
Financial Services

- On June 24th, the Federal Financial Institutions Examination Council (FFIEC) launched a web page on cybersecurity. The web page serves as a resource center for current and future FFIEC-related materials on cybersecurity. This represents another part of the FFIEC’s on-going campaign to “raise awareness of cybersecurity risks at financial institutions and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats that pose risks to all industries in our society.”

- As of July 1, 2014, the U.S. government will start imposing a 30 percent tax on many overseas payments to financial institutions that don’t share information with the IRS as part of the Foreign Account Tax Compliance Act of 2010.

About Cyveillance | Solutions | Blog | Events