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

COME SEE OUR NEW LOOK

If you haven’t visited our website, cyveillance.com, recently, we encourage you to take a look. It’s been newly redesigned from top to bottom with a clean and functional new look. Browse our solutions by industry or function, check out our latest whitepapers and blog posts, and find out what we’ve been up to on social media. We’re extremely proud of the new look and feel, and hope you’ll enjoy it too! Be sure to let us know what you think, and happy browsing.

Top Incidents

Energy

- Molotov cocktails were thrown at the home of a fracking company security guard in Northern Ireland early Sunday night. The victim is an employee of Australia-based Tamboran Resources, a privately-held exploration and production company set to begin exploration near Belcoo, about 95 miles west of Belfast. No one has claimed responsibility.

Agribusiness

- President Vladimir Putin issued a decree that bans or reduces for one year imports of
food and agricultural products from countries that have imposed sanctions on Russia in the crisis over Ukraine.

**Insurance/Healthcare/Pharmaceutical**

- Chinese prosecutors charged a British investigator and his American wife with illegally obtaining private information in a case that could be key to a bribery investigation against GlaxoSmithKline.

**Financial Services**

- A Russian crime ring swiped a database of pilfered login credentials, including 1.2 billion unique username-password combinations and 542 million email addresses, making it the largest known collection of stolen credentials to date. The attackers used a botnet to hunt for sites vulnerable to SQL injection hacks. They compromised roughly 420,000 websites and lifted 4.5 billion username-password combinations in all; after eliminating duplicates, the number drops down to a no-less-impressive 1.2 billion unique login combos. The criminals however have not offered the compromised data for sale, instead it appears that they are currently using them to operate a spammer-for-hire service. Nevertheless, the incident underlines the persistent troubles of lax website security, inadequate monitoring, and single-factor authentication.

**Global Intelligence**

- On 8/6/2014, a Chinese news outlet reports multiple malwares and phishing sites are exploiting the recent earthquake in Yunnan, China. The malwares and phishing sites often contains messages like “latest news of earthquake” and “Donation site for Yunnan Ludian earthquake” to obtain users' online banking account numbers and passwords.

**Legal and Regulations**

- On July 29, 2014, a bipartisan group of congressional representatives introduced legislation that would codify a federal private right of action for trade secret misappropriation. The proposed bill, the Trade Secrets Protection Act of 2014, H.R. 5233 (“the Bill”), would permit companies and individuals to sue under the Economic Espionage Act.

**Energy**

- In the wake of the annual ALEC convention, activists are drawing on the organization’s Jeffersonian Project to draw new comparisons between ALEC and the Nazi Party.

- Portland Rising Tide, which has already conducted at least one disruptive anti-oil train action, has recently penned a column strongly opposed to oil trains carrying Bakken crude.

- French authorities are considering scaling back their smart meter adoption goals. The consumer benefit is not considered strong enough to justify the goals as they stand.

- The group spearheading a blockade of an Enbridge pipeline construction site in southwestern Ontario said Wednesday it will continue the protest until its concerns are addressed. Some 30 activists began their campaign early Tuesday in the community of Innerkip near Woodstock at the site for the pipeline called Line 9. The blockade dubbed Dam Line 9 is aimed at preventing the installation of a valve near River Thames, which the protesters say isn't adequately protected from the risk of a spill.

- Molotov cocktails were thrown at the home of a fracking company security guard in Northern Ireland early Sunday night. The victim is an employee of Australia-based Tamboran Resources, a privately-held exploration and production company set to begin exploration near Belcoo, about 95 miles west of Belfast. No one has claimed responsibility.
• A ‘Memorandum of Understanding' obtained under the Freedom of Information Act shows the high level of collusion between Salford Council, IGas, Greater Manchester Police, Peel Holdings and other organizations during the anti-fracking protests at Barton Moss in the UK – sharing intelligence, communications and branding. The Memorandum also set out the level of force that the police were expected to use, which has led solicitor Simon Pook to question “the violent actions of Greater Manchester Police at Barton Moss”.

• The owner of a Youngstown (OH) oil-and-gas-drilling company was sentenced Tuesday to 28 months in prison for ordering employees to dump tens of thousands of gallons of fracking waste into a tributary of the Mahoning River. U.S. District Judge Donald Nugent also fined Benedict Lupo, 64, of suburban Poland $25,000.

---

**Agribusiness**

• The Organic Consumer’s Association (OCA) is calling on the organic dairy industry to cut ties with the IDFA (International Dairy Foods Association) because it is one of several trade associations suing Vermont over its GMO labeling mandate. In an open letter dated July 23, recipients were asked to take a stand by withdrawing their company's membership from the GMA and/or the IDFA.

• President Vladimir Putin issued a decree that bans or reduces for one year imports of food and agricultural products from countries that have imposed sanctions on Russia in the crisis over Ukraine.

• A federal judge in Utah has refused to toss out the country's first lawsuit challenging an “ag-gag” law that criminalizes undercover investigations of slaughterhouses and “factory” farms.

• Corn output in China may drop for the first time in five years because of drought in the North China Plain, the country’s second-biggest producing region.

• Past polls have shown that Americans overwhelmingly support GMO labeling, they just don’t want to pay for it. That leads to a current challenge – no one’s sure exactly how much it would cost.

• The Environmental Protection Agency is eight months past the deadline for issuing its mandate of how much ethanol, biodiesel and other petroleum alternatives must be blended into motor fuels this year, leaving investors wary about the government’s commitment to the program.

• The Obama administration is moving to cut down on the thousands of foodborne illnesses linked to chicken and turkey each year with an overhaul of poultry plant inspection rules that are more than 50 years old.

• The US Fish and Wildlife Service will be extending its ban on neonicotinoids originally announced for the Pacific coast region. The ban will extend to all national wildlife refuges in the US by 2016- 150 million acres in all. This ban will also include GMOs grown to feed wildlife.

• On August 3, 2014, naturalsociety.com reports that the EU has recently voted to allow member states to decide for themselves whether or not they will allow GMO cultivation. The article states that many worry this will make the EU much more vulnerable to GMO’s.

• On August 3, 2014, naturalsociety.com reports that the EU has recently voted to allow member states to decide for themselves whether or not they will allow GMO cultivation. The article states that many worry this will make the EU much more vulnerable to GMO’s.
On July 31, 2014, 50 members of Congress delivered a signed letter to Thomas J. Vilsack, Secretary of the Department of Agriculture; and Gina McCarthy, Administrator of the EPA. The letter urges the EPA not to approve the Enlist Duo 2,4-D herbicide currently under consideration.

Amendment 1, a state constitutional amendment in Missouri has been passed by a slim margin in the August 5 statewide vote. The amendment will add the right to farm and ranch in the state of Missouri. The amendment passed by only about 2,500 votes. Opponents of the bill are considering demanding a recount.

On August 6, 2014, 64 top scientists from around the country submitted an open letter to the U.S. National Academy of Science’s National Research Council (NRC). The letter criticizes the NRC’s decision to create a panel of scientists to undertake the study “Genetically Engineered Crops: Past Experience and Future Prospects.” According to the scientists opposing the panel, they argue that the panel seems predisposed to support GMO’s and do not include the proper breadth of experience of scientists and farmers to take on the study.

### Insurance/Healthcare/Pharmaceutical

**Insurance**

- While many of the healthcare-related identity theft and other fraud cases that South Dakota and other states are seeing involve insiders at clinics and other organizations, cybercrime is a growing concern.

- Franklin-based Community Health Systems will pay $98 million to settle federal charges that it admitted patients to emergency rooms that didn’t need to be hospitalized.

- A recent update to HHS’s public breach tool shows that Western Regional Center For Brain And Spine Surgery reported a breach affecting 12,000 patients. The breach began on November 28, 2011 until June 29, 2012 and involved “theft, network server.” A letter sent to patients dated July 9, 2014, explains that on or about May 13 of this year, the Las Vegas-based practice received information from law enforcement that there had been a breach of personal health information from their billing files.

- Royal Inland Hospital in Canada has advised 1,628 patients their privacy has been violated. Nancy Serwo, acting administrator at the hospital, said two boxes of records were returned to the hospital on June 16 after they were discovered in a filing cabinet the hospital had donated elsewhere last year. The best estimate of when the equipment was disposed of is last October, Serwo said, though she could not identify who received it. The letter sent to patients states no one asked for identification from the person who returned the boxes to the hospital, which has made it difficult to investigate the breach.

- Two of California’s largest health insurers are partnering to create a massive database of patient medical records. With just a few strokes of a keyboard, doctors and nurses will be able to access the medical histories of about one in four California residents. Supporters say the effort by Anthem Blue Cross and Blue Shield of California could mean faster, cheaper and better healthcare. But the system faces significant technological challenges and privacy concerns.

- Urological Associates of Southern Arizona, according to Tucson News Now, has notified more than 3,000 patients that their data was compromised when labels attached to urine sample cups weren’t removed prior to cup disposal.

- A new study of hospitals shows that, in general, those that routinely use electronic health records don’t submit higher claims for insurance payments than institutions that have yet to fully adopt EHRs.

- An insurance giant Aetna is suing to recover millions of dollars in fraudulent claims.
submitted by a Parsippany diagnostic lab that bribed doctors to refer their patients to the
lab. Aetna Health Inc. and Aetna Life Insurance Co. filed a 45-page civil complaint in
Camden County Superior Court this week against Biodiagnostic Laboratory Services,
three of its owners, and more than a dozen doctors who have admitted pocketing bribes
in return for referring patient blood work to the lab and ordering unnecessary tests.

- The Jersey City Medical Center is notifying patients whose unencrypted protected health
  information was on a CD lost by United Parcel Service in June. The CD contained data
  the center was required to provide to Medicaid, and included patients’ names, social
  security numbers, and for some patients, date of birth, medical record number, gender,
  and information on visits to the Medical Center in 2011.

- Cisco used its 2014 Annual Security Report to offer its perspective and findings on the
  various threats organizations need to be aware of, including distributed denial-of-service
  (DDoS) attacks. The report concentrates on trust, threat intelligence, industry trends,
  and recommendations from Cisco. While most of the analysis is cross-industry, there are
  some interesting pieces of information that would be pertinent to the healthcare industry.

- The U.S. Food and Drug Administration (FDA) has established fiscal year 2015 drug
  facility user fees that have increased 12-15 percent over current rates. The new fees will
  take effect October 1, 2014. Facilities in India, which is the largest source of medicines
to the United States, will pay more than domestic facilities.

Pharmaceutical

- A Manhattan federal judge on Thursday said the U.S. Department of Justice may pursue
  most of its lawsuit accusing Novartis AG of civil fraud for allegedly using kickbacks to
  boost sales of drugs covered by Medicare and Medicaid. U.S. District Judge Colleen
  McMahon allowed the government to continue its False Claims Act case against the
  Swiss drugmaker over claims submitted to Medicare and some state Medicaid programs
  for Myfortic, used by patients with kidney transplants, and Exjade, for patients who get
  blood transfusions.

- Institutional Shareholder Services (ISS) is backing activist investor Bill Ackman’s call for
  a special meeting of Allergan investors that could topple the company’s board and
  increase the chances of a takeover by Valeant Pharmaceuticals International. ISS’
  recommendation on Wednesday follows a similar view from shareholder advisory firm
  Glass Lewis on Monday, giving Ackman’s Pershing Square Capital Management
  momentum as the hedge fund tries to muster support for the meeting. ISS is the largest
  proxy adviser for institutional investors.

- After being rejected by AstraZeneca, Pfizer still has a chance to clinch the drug
  industry’s biggest deal. While Pfizer shelved plans in May to buy the UK company in a
  record transaction, its plan B could be an even larger target, $118bn GlaxoSmithKline,
said Berenberg Bank. A takeover of London-based Glaxo, which has become almost
  10% cheaper in the past two weeks, would give Pfizer a lung-drug business and more
  vaccines. Another possibility, Irish-domiciled Actavis at $57bn, would offer a pipeline of
  new products and generic medicines. Either may allow New York-based Pfizer to move
  its headquarters abroad and lower its tax rate.

- U.S. doctors and teaching hospitals remain unable to review an online federal
government database of payments they have received from drug and device makers,
after a government agency shut it down to investigate a data mix-up. The Centers for
Medicare and Medicaid Services took the so-called “Open Payments” system offline
Sunday night and doesn’t have an estimate of when it will be working again, a CMS
spokesman said Thursday. The data mix-up involved at least one doctor being able to
see the payment data for another doctor whose records were erroneously linked.

- Chinese prosecutors charged a British investigator and his American wife with illegally
  obtaining private information in a case that could be key to a bribery investigation
  against GlaxoSmithKline.

- The World Health Organization may declare an international public health emergency
over Ebola and will convene a panel of experts in coming days to explore the use of experimental treatments.

- The National Association of Boards of Pharmacy was granted the .pharmacy domain. They claim they will use it to provide a “the National Association of Boards of Pharmacy is seeking a .pharmacy domain. Under the Association’s Registry Agreement, executed with ICANN on June 19, 2014, the new .pharmacy generic Top-Level Domain (gTLD) will be available only to legitimate online pharmacies and related entities located in the United States or other countries. The Registry Agreement also includes a number of safeguards intended to protect consumers around the world.” This decision brings with it a lot of controversy.

Financial

Activism

- Housing activists held an anti-eviction protest on August 4th in front of a property management company in Clarkston, GA, demanding management stop evicting renters from their apartments.

- Housing activists in Chicago, IL staged an anti-eviction protest on August 2nd at the home of a local resident facing eviction by a leading regional bank.

- An activist group will hold an anti-eviction protest on August 13th in support of a local resident at her eviction hearing at a district court in Detroit, MI. The group urges its supporter to call the Chicago office of a GSE for housing and demand it let the resident stay in her property.

- Activists launched a petition calling on a leading U.S. bank to meet directly with families affected by the bank’s ‘toxic’ mortgages and the ‘destruction’ of the U.S. economy. Occupy Wall Street is promoting the petition, which consists of more than 6,000 signatures to date.

- National housing groups are planning national actions against the United States Department of Housing and Urban Development (HUD) in several cities on September 9th to demand better housing policies.

- Housing activists will stage an anti-eviction protest at a leading U.S. bank branch in Jersey City on August 21st in support of a local homeowner facing eviction by the bank.

- Occupy Wall Street will conduct an action on September 17th at the Charging Bull in NYC to demonstrate “Money Changers, Lenders, and Politicians” sacrifice of Americans in the name of greed. Protest marches may occur around NYC before participants congregate at the Charging Bull.

- Occupy Wall Street will conduct a “press conference” on September 17th at 1 Liberty Plaza in NYC in commemoration and celebration of the 3rd Anniversary of OWS.

- Housing activists staged protests on August 6th and 7th at the county court in Atlanta, GA in support of the defendants standing trial for preventing the eviction of a local homeowner from his GSE-owned home last year.

- Activists conducted an anti-Wall Street protest march on August 8th through Detroit, MI’s Financial District to several leading U.S bank branches. The same activist group and its affiliates have been staging demonstrations in downtown Detroit every Friday afternoon for the past thirteen weeks.

- Housing activist groups on August 7th held a public discussion in Chicago, IL about the challenges and opportunities homeowners face while “fighting to take back their homes
in Chicago."

- A petition was created at whitehouse.gov to impeach FHFA Director Mel Watt for allowing an illegal net worth sweep and seizure of shareholders profits from the two GSEs for housing.

- Local housing activists will hold an anti-eviction protest on August 14, 2014 in Providence, MA.

- Housing activists in Seattle, WA staged a rally and press conference on August 8th at King County Courthouse in Seattle in defense of a local family facing eviction.

**Information Security Risk**

- Hackers continue to target Israeli banking and financial websites with various cyber-attacks due to the perceived unjust Israeli occupation of Palestine.

- A hacker claimed he previously accessed the systems of a leading U.S. bank and vulnerabilities within the bank’s IT infrastructure still remain exploitable.

- Hackers claimed to have taken down the website of Israel’s largest commercial bank.

- Researchers said the infamous banking trojan, Citadel, has now been enhanced with the ability to exploit a device remotely, and thereby use the system as host to indulge in cyber-crime. Citadel’s enhanced ability comes in the form of Remote Desktop Protocol (RDP) and Virtual Network Connection (VNC). RDP and VNC protocols are widely used the world over by technical support teams to offer remote technical support to users. Similarly, hackers can use Citadel malware remotely to obtain full control of a host computer system. The researchers point out that hackers using the updated Citadel malware get to access host systems via the Remote Desktop Protocol even after the malware has been detected and removed from the host computer. Additionally, Citadel offers the attacker the ability to run Windows shell commands. These commands can come in handy if the attacker wants to get a clearer picture of the network in which the infected PC resides, scan it and prepare the grounds for something more than just fraud.

- Hackers targeted the website of an Australian cause funding platform that allows people to create and donate to fundraisers and charities and stole the credit card details of around 12,000 people. Authorities said some of the credit card details have already been used to make fraudulent transactions in the United States, Europe and the United Arab Emirates.

- Researchers said the much-rumored banking Trojan ‘Kronos’ has appeared in the wild and is targeting French financial institutions by using “Zeus-style web-injects” in HTML and JavaScript to trick the user and carry out fraudulent transactions without the user’s knowledge.

- Industry experts claim that DDoS attacks are rising in number and volume as a result of the Israel-Hamas conflict. Researchers detected a rise in the number of DDoS attacks targeting Israel in the first week of July, going from an average of 30 attacks per day to an average of 150 attacks initiated per day in July — peaking at 429 attacks on July 21st. Linking these cyber-attacks to political situations, June 30th is when Israel publicly attributed the deaths of three kidnapped Israeli teenagers to Hamas, and on July 7th, “Operation Protective Edge” was launched by the country. As the political conflict raged on, so did the frequency of DDoS attacks until a drop occurred on July 28th lasting through August 2nd. The drop in attacks roughly correlates with cease fire talks which began July 27th. From July 28th through August 2nd, there were 192 attacks recorded in total. On August 3rd, the number of DDoS attacks rose sharply, with 268 attacks in total. In addition to the number of DDoS attacks over these time periods, the security researchers also noticed an increase in the peak size of these attacks. In June, no attacks exceeded 12Gbps. In July, seven DDoS attacks exceeded this size, with the largest peaking at 22.56Gbps on July 12th. When cease-fire talks fell apart on August 3rd, the largest DDoS attack was recorded at a size of 29Gbps. The duration of DDoS...
attacks has also increased. In June, the average duration was 20 minutes — with a peak duration of 24 hours — and in July, the average duration was 1 hour 39 minutes.

- According to a new report, the Backoff malware has already infected point-of-sale (POS) systems at 600 U.S. retailers since October, 2013. Some of the 600 retailers are large retail chains, and all of the retailers identified as being infected with the malware are aware of the breach, said the report. The hackers target businesses that use remote desktop applications. Once infiltrated, Backoff then scrapes memory from the victims’ machines, searches for track data and logs keystrokes to reap sensitive data such as credit card information. When the malware sees a credit card system in memory, or typed in, it grabs that credit card information, then encrypts it and ships it out to another system under the criminals' control.

- The website of an e-commerce business specializing in mobile accessories and unlocked cell phones was compromised by malware and the personal information of an undisclosed number of customers, including payment card data, may have been leaked. The incident was discovered on July 1. The malware could have compromised the information for customers who made purchases between Dec. 24, 2013, and Jan. 19.

- A Russian crime ring swiped a database of pilfered login credentials, including 1.2 billion unique username-password combinations and 542 million email addresses, making it the largest known collection of stolen credentials to date. The attackers used a botnet to hunt for sites vulnerable to SQL injection hacks. They compromised roughly 420,000 websites and lifted 4.5 billion username-password combinations in all; after eliminating duplicates, the number drops down to a no-less-impressive 1.2 billion unique login combos. The criminals however have not offered the compromised data for sale, instead it appears that they are currently using them to operate a spammer-for-hire service. Nevertheless, the incident underlines the persistent troubles of lax website security, inadequate monitoring, and single-factor authentication.

- According to a recent security report, the amount of credit card fraud across 19 European countries (including Russia) was worth €1.55 billion. France had the highest rate of fraud in terms of the amount of losses caused by fraud per card transaction, followed by Greece and the UK. However, in terms of overall losses, the UK was harder hit with losses totaling €535 million. France came next with €429 million losses. In terms of the increase in France compared to 2012, the country saw just a slight jump of 1 percent, compared to 16 percent in the UK and 27.6 percent in Russia. Together the UK and France suffered 62 percent of the total losses caused by card fraud among the 19 countries that were studied.

**Legal, Litigation, Regulatory Risk**

- Housing activist group members met with the U.S. Attorney for the District of Colorado to discuss ongoing settlements between the Department of Justice and big banks across the country for fraud in representing their residential mortgage backed securities. Members shared how they have seen people foreclosed on using the very methods the big banks agreed to stop in previous settlements. Members of the group were promised and later given the name of the individual who oversees compliance with the settlements referred to and encouraged to share stories of people who have experienced these continued fraudulent foreclosures and to come back to the table with the Attorney if they didn't gain traction in their efforts.

- A former employee at a Chicago-based investment firm pleaded guilty to stealing data from the company and high-frequency trading computer code from another organization. The 26-year old who was first charged in 2011, recently admitted taking the proprietary information from his employer that year and to an earlier theft of trade secrets from an unnamed company based in Red Bank, New Jersey, that developed HFT infrastructure software.

**Operational Risk**

- Bidding is underway to build a powerful computer to give federal regulators a fuller view of the way the market works. The Consolidated Audit Trail, or CAT, will be one of the
largest databases in the world, designed to funnel 50 billion daily records into an archive. The computer will track every stock quote, order, and trade, including when and where transactions occur, the brokers who handle them, and the customers they represent. The CAT will pull data from the 18 U.S. public stock and options exchanges and the private trading venues run by banks, known as dark pools, that don’t have to immediately report data to the SEC. If it works as planned, the CAT will improve the SEC’s ability to scrutinize parts of the market it can already see and shine a spotlight on the places it currently can’t. More than 30% of trading occurs outside the SEC’s field of view, either in dark pools or inside large wholesale brokerages that match buy and sell orders internally. The computer will be able to flag suspicious patterns suggesting insider trading. The SEC is allowing the public financial exchanges and FINRA to run the bidding process that will choose a company to build the CAT and decide how much to spend on it.

- Researchers uncovered a series of incidents in which a bitcoin thief redirected a portion of online traffic from no less than 19 Internet service providers with the goal of stealing cryptocurrency from a group of bitcoin users. Though each redirection lasted just 30 second or so, the thief was able to perform the attack 22 times, each time hijacking and gaining control of the processing power of a group of bitcoin miners, the users who expend processing power to add new coins to the currency’s network. The attacker specifically targeted a collection of bitcoin mining “pools”–bitcoin-producing cooperatives in which users contribute their computers’ processing power and are rewarded with a cut of the resulting cryptocurrency the pool produces. The redirection technique tricked the pools’ participants into continuing to devote their processors to bitcoin mining while allowing the hacker to keep the proceeds. At its peak, according to the researchers’ measurements, the hacker’s scam was pocketing a flow of bitcoins and other digital currencies including dogecoin and worldcoin worth close to $9,000 a day.

**Reputational Risk**

- An article published last week claimed the concentration of fertile agricultural land in fewer and fewer hands is directly related to the increasing number of people going hungry every day. The article noted that institutional investors, including hedge funds, private equity, pension funds and university endowments are "eager to capitalize on global farmland as a new and highly desirable asset class.

- An op-ed published last week claimed the two GSEs for housing “have to go” because they played a leading role in setting up the housing market for its big fall by encouraging lending to unqualified borrowers. The publication argued that the GSEs helped set up many families to fail, and their continued existence gives lenders an incentive to make riskier loans than they would if the government weren’t providing guarantees.

**Global Intelligence**

**China**

- At least 75 people were killed from an explosion at Zhongrong Metal Products Ltd. Co, a Taiwan-based wheel hub-polishing factory in Kunshan, early Saturday morning. 180 people were injured from burns and respiratory damage from smoke inhalation. The initial investigation indicated that the blast was caused by the ignition of metallic dust particles in the workshop.

- On 8/8/2014, a Chinese news outlet reports the Chinese government official are advised to give up using Apple products due to its system backdoor.

- On 8/8/2014, a Chinese news outlet reports the discovery of a security vulnerability on most mobile devices’ ODM system for software updates. The vulnerability on ODM system could be exploited by cyber criminals to gain control of mobile devices remotely.

- On 8/8/2014, a Chinese news outlet reports a new malware are current spreading in the
United States, Europe and Russia infecting 500 thousands android devices. According to the article, the malicious application could gain control of Root, and ultimately gain complete control of the mobile device.

- On 8/6/2014, a Chinese news outlet reports a trading platform of NextCoin and BitCoin, DGEX experienced a security breach and lost 52 BitCoin and 1.2 million NextCoin.

- On 8/7/2014, a Chinese news outlet reports a new malware targeting Android devices disguised as Facebook application for Android to lure users to download. Once user has downloaded and installed, it will send out text message and makes unauthorized phone call. In additional, it also collect users text messages, contacts, call logs, picture, documents and etc.

- On 8/6/2014, a Chinese news outlet reports multiple malwares and phishing sites are exploiting the recent earthquake in Yunnan, China. The malwares and phishing sites often contains messages like "latest news of earth quake" and "Donation site for Yunnan Ludian earthquake" to obtain users' online banking account numbers and passwords.

- On 8/5/2014, a Chinese news outlet report a server of the liver care center of The Chinese University of Hong Kong suspects to have experienced a security breach and exposed more than 10 thousand patients' personal information.

- On 8/4/2014, a Chinese news outlet reports the result of Arbor Network's research on world wide DDoS attacks over the first half of 2014.

- On 8/5/2014, a Chinese news outlet report China Telecom's DNS server in Shaanxi, China experienced a hacker attack and hijacked Baidu's domain name. The user is Shaanxi China find that when they enter Baidu's domain name, they will be redirect to a dnserror webpage.

**Germany**

- 160,000 homes in Berlin lost Internet, TV, and phone service for a day after unknown attackers cut 400 fiber optic cables inside a cable tunnel last Sunday. Police does not rule out a political motivation for the attack. The police department charged with the protection against political extremism (Staatsschutz) is investigating the incident.

**North America**

- On 8/2/2014 ABC News 7 reported that the Philadelphia man has been sentenced to 3 to 6 years in state prison for masterminding a scam that cost Comcast $2.4 million in lost revenue.

- On 8/5/2014 CNet reported that Russian gang hacked into more than 420,000 web and FTP sites, amassing usernames and password combinations and millions of email addresses.

- On August 7th, several hundred protesters rallied outside of CNN's Time Warner headquarters in New York to demonstrate outrage over its coverage of the conflict in Gaza. The rally, titled "#StandWithIsrael" believes that the journalism covering the conflict between Israel and Palestine is slanted in Palestine's favor. #StandWithIsrael also held a rally in Boston and is expected to continue its presence as the conflict continues.

- E-commerce site WirelessEmporium.com experienced a customer data breach which occurred between Dec 24, 2013 and January 2014. In addition, the hacker may have acquired customer information including their names, addresses, payment card numbers, card expiration dates, and CVV codes.

- The Backoff malware, detailed in a US-CERT alert on Friday, has already infected point-of-sale, or POS, systems at 600 retailers, according to security firm Trustwave. The Backoff malware is able to infect POS systems through remote desktop software used by retailers to enable remote workers to access their corporate networks.
Wearable technology like Google Glass has raised privacy concerns and that has some tech companies rethinking design approaches.

A European team demonstrated a whole panoply of successful attacks against HTTPS, which is supposed to secure your web browsing. Most notable are a “Cookie Cutter” attack which steals users’ cookies, letting the attacker hijack sessions on any supposedly-secure site, and a way to impersonate–again, over HTTPS–any site hosted by the Akamai content delivery network.

President Barack Obama spoke in favor of net neutrality this week, pushing back against the idea of paid prioritization, which many call Internet “fast lanes.” Following the president’s comments, a number of technology companies joined cultural and privacy groups in praising the American leader.

**Malaysia**

- On 8/5/2014, a Malaysian news outlet reports flash mob gathered outside of a McDonald restaurant in Perak Malasia, calling to boycott Israel, in support of Gaza.

- On 8/7/2014, a Malaysian news outlet reports the revenue of McDonald restaurants in Kerteh and Dungun, Malaysia declined by 80 percent due to boycott to protest against McDonald’s association with Israel.

- On 8/7/2014, a Malaysian news outlet reports 56 employers will face action for failure to comply with minimum wage order implemented in 2012.

- On 8/2/2014, a Malaysian news outlet reports Human Resources Deputy Minister said that private sector employers should provide incentive for their employees who work on public holiday such as Aidilfitri.

- On 7/31/2014, a Malaysian news outlet reports MTUC wins a landmark case for minimum wage in the hotel industry.

- On 8/2/2014, a Malaysian news outlet reports a protest at Merdeka Square in Kuala Lumpur against Israel’s assault on Palestine.

**Vietnam**

- On 8/7/2014 the International Business Times reported that an app that allows users to search for a product linked to targeted companies or countries in order to boycott them has seen a surge in users signing up to anti-Israel campaigns. Between Long Live Palestine Boycott Israel and Avoid Israeli Settlement Product have close to 350,000 supporters, over a quarter of which have joined in the last 12 hours (at the time of publication).

- On 8/6/2014 the National Law Review reported that last month, the EEOC issued new Enforcement Guidance on pregnancy discrimination in the workplace and related issues. The EEOC clarified how Title VII and the ADA interact to protect pregnant employees. The new guidelines prohibit employers from forcing pregnant workers to take leave and acknowledge that “employers may have to provide light duty for pregnant workers.” After childbirth, lactation is now covered as a pregnancy-related medical condition. The article contains no commentaries.

- On 8/6/2014 the Wall Street Journal reported Apple claimed that roughly 500,000 jobs have been created in Europe that are directly attributable to the App Store. Of the more than $20 billion developers have earned from App Store sales worldwide, $6.5 billion has been paid to European developers.

- On 8/7/2014 Lao Dong News reported that Vietnam’s National Wage Council met and voted on raising the national minimum wage by 15.1%. This is only a proposal by the National Wage Council, the final proposal will be presented by the government in September. According to the article, the LDLDVN, Vietnam’s only official union, is unhappy with this proposal because it will only cover 75% of the minimum cost of living. The National Wage Council stated that minimum wage will have to be raised to
accommodate the minimum cost of living by year 2017. In that case, in the coming 2 years, minimum wage will have to be raised an average of 12% each year.

- On 8/4/2014 Info.VN, a local VNese media site, reported that the central coastal city of Da Nang has officially covered its territory with Wi-Fi signal after a year-long trial. The Wi-Fi service will be provided for free at least until the end of 2016 and then the city will charge the users who want to improve their internet line quality.

- On 8/5/2014 India Briefing reported that in a landmark decision, India's Union Cabinet approved a proposal to amend 3 key labor laws including the Factories Act 1948, Apprentices Act 1961, and Labor Laws Act 1988. The article goes on to describe the content of these new Acts.

- On 8/4/2014 Global Post reported that South Korean companies advised employees not to visit parts of Africa that have been hit by the latest Ebola virus outbreak. Samsung Heavy Industries, Hyundai Heavy Industries Co. and Hyundai Motor Co. have said they are keeping close tabs on the latest health development. Samsung has ordered on-site employees to take extra precaution in personal hygiene and not to travel to neighboring countries such as Liberia.

- On 8/1/2014 the Journal reported that the union group at Irish Rail announced that it will hold a two-day work stoppage starting Sunday, 8/24/2014, if the company pushes ahead with pay cuts. Further one-day stoppages have been proposed for 9/7/2014 and 9/21/2014.

- On 8/5/2014 Inside Counsel reported that LinkedIn paid nearly $6 million in back wages and damages to 359 current and former employees who were not properly paid overtime between 2/2012 and 2/2014. The company must also inform managers about proper overtime pay regulations and protect against retaliation towards those who raise workplace issues.

- On 8/1/2014 Business Times, a local VNese media source, reported that the CEO of Intel Products in Vietnam announced that 80% of Intel's chips used in computers around the world will be made by Intel plant in Vietnam by this time next year. Intel Product Vietnam has more than 1,000 local employees and it took them only 2 months to be certified to produce Haswell processors. The VNese plant is making two of Intel's flagship products, the SOC and the Haswell CPU.

- On 8/1/2014 Thanh Nien News, a local VNese media source, reported that the head of Vietnam's only labor union warned that a pledge to ensure an equitable minimum wage by 2017 will fail unless authorities hike it by at least 23% next year. Dang Ngoc Tung, chairman of Vietnam General Confederation of Labor proposed the minimum wage be increased to 2.3-3.4 million VND a month. Many companies in Hanoi and Ho Chi Minh City already pay workers between 2.9-3 million apart from allowances and bonuses. The National Wage Council will wrap up a plan on minimum wage increases for 2015 this month and submit it to the central government for approval in September.

- On 7/28/2014 Business Times, a local VNese media source, reported that more than three months since it was put into operation, the Samsung Electronics Vietnam Thai Nguyen earned nearly $2 billion USD from exports, mostly smartphones and tablets (June statistics).

Argentina

- Workers of software company Sonda went on an indefinite strike in Argentina after the company failed to answer to their demands. The workers' demands are: increase in wages, better working conditions and fair treatment to the workers.

Legal and Regulations
Gov. Lincoln D. Chafee of Rhode Island recently signed the 2014 Student and Employee Social Media Privacy Acts into law. Under this new law, employers cannot 1) require an employee or applicant to disclose social-media information, including their username, password, or other means of access to an account; 2) require or compel an employee or applicant to add someone to their list of contacts associated with a social-media account as a condition of employment; or 3) discharge, discipline, or penalize an employee for refusing to divulge social-media information to the organization. The law also creates a private right of action for employees to sue their employers seeking declaratory relief, damages, and attorneys' fees.

On July 29, 2014, a bipartisan group of congressional representatives introduced legislation that would codify a federal private right of action for trade secret misappropriation. The proposed bill, the Trade Secrets Protection Act of 2014, H.R. 5233 (“the Bill”), would permit companies and individuals to sue under the Economic Espionage Act.