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
- Pharmaceuticals
- Retail
- Technology
- Telecommunications
- Defense
- Law Enforcement

Cyber Safety Awareness Training

Protect your Organization with Computer-Based Training

Are your employees the weak link in your security program? We want to help you educate your employees to keep them — and your organization — more secure.

Our computer-based cyber security training can help your employees learn how to protect your organization from the latest threats and reduce the high costs associated with incident remediation.

Top Incidents

Energy

- The Cuomo administration announced that it would ban hydraulic fracturing in New York State, ending years of uncertainty by concluding that the controversial method of extracting gas from deep underground could contaminate the state’s air and water and pose inestimable public-health risks.

Agribusiness

- The wheat industry continues to be affected by a very large cold airmass through North American in the middle part of November while wheat was still being planted and
emerging. Additionally, logistics remain a major concern for the grain industry this winter.

**Insurance/Healthcare**

- The newly approved fiscal 2015 federal budget includes no increase in funding for the federal agencies responsible for enforcing HIPAA and setting policies and standards for the HITECH Act financial incentive program for electronic health records.

**Financial Services**

- The Federal Bureau of Investigation officially placed blame for the crippling hack of a major film studio arm of a Japanese electronics conglomerate on North Korea. The FBI cited technical analysis that found lines of code and signature data that implicated the nation state.

**Global Intelligence**

- On December 18, 2014 Business Standard reported Foxconn has informed its workers they do not have to come to the factory in Siperumbudur, India for work from December 22, 2014 as the company was planning to suspend operations. According to the workers, the company so far has sent around 1,000 workers on leave with salary from a total 1,700 employees.

**Legal and Regulations**

- The National Institute of Standards and Technology (NIST) recently released an update on its Framework for Improving Critical Infrastructure Cybersecurity (The Framework). The Framework was first issued in February 2014 as a voluntary risk-based program to enable owners and operators of U.S. critical infrastructure to assess and remediate their cybersecurity risks. NIST welcomes ongoing feedback via email at cyberframework@nist.gov. It is soliciting input as to how organizations are using the Framework, and requesting specific suggestions for improvement and for possible outreach activities.

**Pharmaceuticals**

- In early November, the FBI and Europol announced ‘Operation Onymous’ – a joined-up international law enforcement action which saw the take-down of hundreds of dark markets on anonymous networks like Tor. These websites – which included Silk Road 2.0 - were selling illegal goods including weapons, drugs and hacker tools. However a report recently uncovered by SCMagazineUK.com sheds some doubt on how effective this action has been, with most darknet sellers, advertisers and buyers moving onto new – or undisturbed – market places.

**Retail**

- Holiday shopping is up 15% from last year to $42.5 billion, according to a new comScore report. At least $1 billion of those figures came from online desktop sales. Additionally, retail cyber security remains a priority for companies in light of data breaches at Target, Home Depot, Neiman Marcus and others in the past couple years. Chief Information Security Officers (CISO) positions have become more common in retail companies’ senior leadership teams.

**Technology**

- TechWeb China reported that several former Sony Mobile employees demonstrated with protest signs and banners outside of the company’s mobile division headquarters in Beijing over layoffs which will allegedly impact 700-800 Sony Mobile (China) employees. Sony stated that the layoff plans have not been finalized and that they will make efforts to provide compensation and job transition assistance to laid off personnel.
Telecommunications

- The hacking attack on Sony Pictures may have been a practice run for North Korea's elite cyber-army in a long-term goal of being able to cripple telecoms and energy grids in rival nations, defectors from the isolated state said.

Defense

- The experts from Kaspersky Lab’s Global Research and Analyst Team have compiled a list of top emerging threats in the APT world for 2015 which includes fragmentation of largest APT groups, targeting executives through hotel networks, enhanced evasion techniques, and new methods to exfiltrate data. APT groups will evolve to become stealthier and sneakier, in order to better avoid exposure.

Law Enforcement

- Big-city police departments and union leaders around the country are warning the rank and file to wear bulletproof vests and avoid making inflammatory posts on social media in the days after a man ambushed two officers and shot them to death inside their patrol car. The slayings of Officers Rafael Ramos and Wenjian Liu on Saturday afternoon in Brooklyn heightened fears about the safety of law enforcement officials nationwide, though there is no evidence any threats are imminent. The gunman, 28-year-old Ismaaiyl Brinsley, had vowed in an Instagram post to put "wings on pigs" as retaliation for the slayings of black men at the hands of white police.

Energy

- The European Union will widen its ban on investment in Crimea to target Russian Black Sea oil and gas exploration, EU officials said on Wednesday, tightening sanctions first imposed over Moscow's annexation of the region. At a summit on Thursday and Friday in Brussels, EU leaders meeting in the European Council will announce the punitive measures that are also expected to be coordinated with similar steps by the United States. The investment ban, the latest in a series of measures since July, is also designed to show that despite a dive in the Russian rouble's value, there will be no lifting of sanctions unless Moscow drops its support for rebels in eastern Ukraine.

- A final report by independent researchers shows the radiation leak from the federal government's underground nuclear waste repository in southern New Mexico was small and localized. The report released Thursday by the Carlsbad Environmental Monitoring and Research Center also says no negative health effects are expected among workers or the public. The center is associated with New Mexico State University. Its technicians have been collecting samples since February, when a container of waste from Los Alamos National Laboratory ruptured after being placed in a storage room at the Waste Isolation Pilot Plant. Sampling stations at and near the plant confirmed the presence of trace amounts of americium and plutonium.

- Austrian premier Werner Faymann protested at the British inclusion of landmark nuclear energy projects – including Hinckley Point – within its list of infrastructure eligible for funding under the proposed €315bn Juncker investment plan. The UK has listed several nuclear-related projects within the Juncker plan, a list of 2,000 projects drawn from across all member states, which will be considered for funding under the investment plan.

- The Huffington Post reports that Quebec Premier Philippe Couillard says he is not interested in exploiting the province's shale gas reserves. He tells the CBC's French-language service that Quebecers are largely against hydraulic fracturing. Couillard made the comments shortly after Quebec's environmental review board concluded the environmental and social risks associated with hydraulic fracturing, or "fracking,"
outweigh the financial benefits.

- A group of activists with Portland Rising Tide interrupted business at the Vancouver office of Kinder Morgan to deliver a ‘People’s Restraining Order’ against the company’s plans to expand the Trans Mountain tar sands pipeline in British Columbia.

- A group of New Englanders from FANG (Fighting Against Natural Gas) were arrested for occupying and shutting down the offices of Spectra Energy to protest the company’s plans to expand a network of fracked gas pipelines in the region. The group deployed multiple banners demanding funders divest from Spectra Energy due to the impacts of the company’s projects to local communities and the climate, with one of them hanging from a 24 foot tripod and refusing to leave. “As long as Spectra is committed to the business of devastating local health and the climate, we’re committed to disrupting their business.”

- On December 15, 2014 more than a dozen affiliates of Enbridge and the Tar Sands have been locked out of their workplaces throughout Ontario. Individuals in 9 cities have participated. Doors to banks, political offices, and other institutions associated with Enbridge have been locked or otherwise disabled, with “Closed for Risky Business” notices posted. These notes all convey the same message: “Good people cannot simply watch as the government and big business dismantle protections and poison our communities for profit, so today we call attention to companies that enable Enbridge to continue destroying for profit – their financiers and contractors; their facilitators and publicists. Those who manage their security and their planning, approve their permits and projects – and any other players who passively take part in eco-destruction while operating business as usual.”

- Canadian energy delivery company Enbridge Inc. has temporarily shut down and isolated one of its crude oil pipelines that connects to the United States after a 1,350-barrel, or 56,700-gallon oil spill, the company reported Wednesday evening.

- The Cuomo administration announced that it would ban hydraulic fracturing in New York State, ending years of uncertainty by concluding that the controversial method of extracting gas from deep underground could contaminate the state’s air and water and pose inestimable public-health risks.

- About 40 people were arrested Tuesday for protesting the expansion of a gas storage facility near Seneca Lake, NY. The arrest follow a series of protests over the past month.

- The number of insolvencies of UK oil and gas services companies has tripled in the last year, and the sudden plunge in crude prices is creating financial stress across the sector, according to figures published last week. Accountancy and consultancy firm Moore Stephens said 18 businesses became insolvent in the 12 months to 30 September, against just six the year before. The most powerful nations in Opec are willing to push prices as low as $40 a barrel in their bid to take on Russia and US shale, according to a high-profile Gulf oil minister. Suhail al-Mazrouei, energy minister of the United Arab Emirates, said that the organisation will let prices fall by more than $20 per barrel before they consider an emergency meeting to cut production.

**Agribusiness**

- The wheat industry continues to be affected by a very large cold airmass through North American in the middle part of November while wheat was still being planted and emerging. Additionally, logistics remain a major concern for the grain industry this winter.

- Social media outlets reported that Ft. Lauderdale, FL recently voted yes on the local resolution to support statewide labeling of Genetically Modified Organisms.
Food Business News reported that Cargill will begin a “mass layoff” in Memphis this February. The announcement follows another from September, stating the company would close its Memphis, TN corn milling facility by January 2015.

Potato Business News reported that TNA, a food packaging and processing solutions company, underlined the importance of the Middle East region the company’s global business strategy by launching an Arabic language website.

Fox Business reported that Archer Daniels Midland says it has agreed to sell its global cocoa business to Olam International for $1.3 billion. The agribusiness company says the deal would let it invest in less volatile businesses or distribute money to shareholders, or both.

At the end of annual trade consultations, officials from China and the United States say they will give attention to their approval processes for genetically engineered crops. The meeting in Chicago was punctuated by China’s announcement that it will accept imports of Syngenta's MIR 162 corn, approved for cultivation in April 2010 by USDA.

The Permanent People's Tribunal have called for a ban on GM maize cultivation in Mexico. The Tribunal took into account research gathered over three years from over 1,000 organizations in writing its decision. Efforts supporting GMO cultivation have been stalled by a moratorium and propositions are currently under legal review.

On December 15, 2014, the Center for Food Safety (CFS) harshly criticized the USDA's Environmental Impact Statement on Monsanto's dicamba-resistant soy and cotton. The CFS claims that approval of the new dicamba-resistant crops would increase the herbicide use in the US by 10-fold. The EPA is currently considering the approval of dicamba for commercialization. The CFS has vowed to pursue "all available legal options" to oppose the crops.

On December 17, 2014, the Hawaii County Council voted in favor of appealing a federal court's ruling which overturned the county's Ordinance 13-121 which banned the growing of GMO crops. The case will now move to a higher appeals court.

On December 17, 2014, the Facebook group "GMO Free Florida (Genetically Modified Organisms)" posted about GMO labeling initiatives in Fort Lauderdale, Florida. According to the post, the city of Fort Lauderdale just voted yes on a local resolution to require GMO labeling.

On December 18, 2014, the Facebook group "GMO Free Florida (Genetically Modified Organisms)" posted about an initiative instituted by the mayor of Hollywood, Peter Bober to offer GMO-free snacks in city vending machines.

Chinese approval of Syngenta's genetically engineered corn "increases the likelihood the seed maker will pay settlements" to farmers and exporters who sued over lost export sales, according to lawyers.

The highly pathogenic H5N8 avian influenza virus was confirmed in a backyard poultry flock in Winston, Oregon, said USDA in a "stakeholder announcement." It was the second U.S. discovery of the H5N8 virus within a couple of days.

Normalization of U.S.-Cuba relations, announced by President Obama, will include easier terms for selling U.S. food and agricultural equipment to the island nation, long viewed by farm groups as a natural and nearby market. A White House official called normalization the most significant change in Cuba policy in half a century.

Insurance/Healthcare
Boston Children’s Hospital (BCH) has agreed to pay $40,000 and take steps to prevent future security violations following allegations related to a data breach that affected patient information.

The newly approved fiscal 2015 federal budget includes no increase in funding for the federal agencies responsible for enforcing HIPAA and setting policies and standards for the HITECH Act financial incentive program for electronic health records.

Consumer Watchdog recently urged consumers to opt out of the new electronic health information exchange, Cal INDEX, that is being set up by Blue Cross and Blue Shield until key questions about patient privacy are answered. The nonpartisan, nonprofit public interest group added that the best way to protect privacy when sharing patient information is an opt-in approach.

On September 17, 2014, Reeve-Woods Eye Center in California's information technology consultant discovered that unknown individuals had breached the Eye Center’s server and installed malware on two computers, one at each facility. The malware was capturing screenshots which included patients’ protected health information.

A review by the Information and Privacy Commissioner of Ontario (IPC) of two significant privacy breaches involving the sale of new mothers’ personal health information for financial gain has determined that Rouge Valley Health System (hospital) failed to put in place reasonable technical and administrative safeguards to protect patient information.

A former Alabama hospital worker has been sentenced to serve two years in prison for his role in an identity theft case that led to federal tax refund fraud. The case also has resulted in a class action lawsuit. The breach at 235-bed Flowers Hospital in Dothan, Ala., spotlights the challenge of insider threats and confirms that policies, procedures and training may have little impact on employees who are considering using information for criminal purposes.

The healthcare sector has a big problem. There’s a great deal of information security immaturity and a lack of resources among smaller clinics, rural hospitals, and other organizations. In the push to exchange electronic patient data nationwide, those entities are potential weak links in the security chain. More has to be done to ensure these smaller organizations are aware of emerging cyberthreats and vulnerabilities - and are prepared to mitigate them.

The Department of Health and Human Services is reassessing how its many internal agencies, and the entire healthcare sector, can boost cyberthreat intelligence sharing and analysis as more patient records are digitized and shared.

Financial

Financial Services

Activism

Activists held a protest at an American financial holding company’s regional headquarters in Pasadena, CA on December 16th due to the firm’s intended acquisition of a regional bank in Southern California. Protesters stated the acquisition would form another “too big to fail” bank.

Housing activists urged supporters to create holiday cards intended for the Director of the Federal Housing Finance Agency from which to tell him to reduce principal on underwater mortgages through the two GSEs for housing. The holiday cards will be delivered at a meeting attended by the Director in January 2015.
- Housing activists held an anti-eviction protest in Springfield, MA on December 17th in support of a local resident facing eviction from her bank-owned home.

- Housing activists held a rally at the regional office of the Department of Housing and Urban Development's (HUD) in Atlanta, GA on December 18th. Activists presented HUD with a “Grinch of the Year” award and demanded reforms to the Distressed Asset Stabilization Program (DASP).

- In response to a major bank’s role in recently passed legislation that repealed portions of the Dodd-Frank Wall Street reform act, several activist groups held a protest at the bank’s New York City headquarters on December 18th.

- Anti-foreclosure activists claimed to have successfully stopped “another attempt to re-evict” a local resident from her bank-owned home in Chicago, IL on December 15th.

- An anti-austerity grassroots group based in Liverpool, UK assembled an emergency blockade and successfully prevented the eviction of a family from their home in Bootle, UK.

- NYC’s grassroots community, to include Occupy Wall Street, are conducting nightly “die-in” protests at Grand Central Station in NYC until December 31st from 6:00pm to 10:00pm EST. Additionally, a ‘People’s Monday’ action calling for justice for Eric Garner and Akai Gurley also occurs every Monday at Grand Central Station starting at 7:00pm EST.

- A group of community lenders joined forces to request that the U.S. Government revisit the terms of the two GSEs’ bailout agreements. The group urged the government to take immediate action to “cure” the under-capitalization of the GSEs by re-amending the payment terms established when they were forced to take a bailout after the crash.

- An activist group is urging a NYC-based university to divest from companies that profit from Israel’s ongoing occupation and “illegal” settlement of the West Bank and East Jerusalem.

- A Boycott, Divestment and Sanctions (BDS) activist group against Israel conducted its annual ‘Anti-Apartheid’ Caroling event on December 20th in NYC.

**Information Security Risk**

- The Federal Bureau of Investigation officially placed blame for the crippling hack of a major film studio arm of a Japanese electronics conglomerate on North Korea. The FBI cited technical analysis that found lines of code and signature data that implicated the nation state.

- Anti-Bashar Ul Assad hackers hacked and defaced five websites of a leading U.S. investment bank headquartered in Minneapolis, Minnesota.

- Hackers published a post containing the full account information and partial credit card numbers of consumers who had accounts with a New York Airport WiFi Service. The hackers claim over two million accounts were compromised.

- Hackers claim to be in possession of thousands of accounts of a popular American digital wallet based e-commerce service.

- A new banking Trojan called “TSPY_BANKER.YYSI” is targeting banks in South Korea by using a popular social media site as its command and control system. The Trojan is able to redirect victims to the phishing pages only if they use Internet Explorer to access banking sites. Malware authors are taking advantage of a South Korean law that requires Korean Internet users to access online banking services and make purchases only with Internet Explorer. Official statistics show nearly 75% of all Korean users exclusively use the browser.
A new study said that half of UK and US firms suffered some form of DNS-related attack in the past year, leading to data loss and business downtime. The study interviewed 300 IT leaders across the two countries and found that 76% said they had suffered a DNS attack at some point in the past, with DDoS (74%), DNS exfiltration (46%), DNS tunnelling (45%) and DNS hijacking (33%) the most common. Over half said they lost “business critical data” or revenue while a third said sensitive customer information was lost in the attack. Customer retention and brand reputation were touted as the biggest concerns following an attack, but worryingly in the UK, almost a quarter of respondents (23%) said they didn’t know if their organization had ever suffered an attack.

A review of UK banking websites by using a free SL/TLS scanning tool offered by a Redwood Shores, California-based security firm shows that many UK banks are vulnerable to the POODLE(Padding Oracle On Downgraded Legacy Encryption) security flaw.

The ATM bank cards of roughly 3,000 customers of a regional bank in Virginia were deactivated after a series of skimming incidents. The bank said the thieves were stealing people’s ATM cards and pin numbers by putting a device on the ATM machine that records that information. The thieves are then able to create fake ATM cards to withdraw money.

Multiple financial institutions said they saw a pattern of fraud that indicated an online credit card breach hit an Atlanta, GA-based offsite airport parking service that allows customers to reserve spots in advance of travel via an Internet-based reservation system.

Researchers reported a new phishing campaign is going around that uses Word documents and macros to spread information-stealing malware. With a subject line that says, “Financial Statement,” the email informs the user that his or her requested statement is attached—followed by a confidentiality clause that’s intended to add an air of legitimacy. It carries a malware that is capable of copying contents from the clipboard, as well as logging keystrokes. The data is then posted back to the attackers’ domain.

Researchers said a vulnerability known as Grinch Bug in Linux operating systems can be exploited to give hackers root access to computer systems. The flaw resides in the authorization system in Linux which allows privilege escalation through the wheel. A wheel is a user account with special administrative rights in a UNIX system and controls the SU command, which allows the elevation of the current user to a super user. A hacker could exploit the Grinch vulnerability by either modifying the registered user account in a wheel or by manipulating the Policy Kit (Polkit), a graphical User Interface for managing privileged operations for ordinary users.

Researchers said that malicious actors are targeting mobile devices such as smartphones with remote access Trojans and phishing techniques. Users of iOS and Android devices are at risk of unknowingly installing the Xsser mRAT, a remote access Trojan. Phones infected with the remote access software could be used for surveillance, stealing of login credentials, launching distributed denial of service (DDoS) attacks, and more.

A new study warned that the sophistication of crimeware-as-a-service, an underground business model that pushes adaptable malware from a botnet, rather than simply infecting a single machine is increasing rapidly. In the new report, researchers focused on the banking malware strain known as Vawtrak, which compromises commonly used URLs by injecting them with code. This allows the hackers to steal online banking credentials as they are entered on the bank’s website. Vawtrak is formerly known as Gozi, a name adopted by the Vawtrak operation for their malware. But unlike Gozi, Vawtrak ranks as the “single most dangerous threat” among botnet-based cybercrime malware strains on the market today.

Domain-name overseer ICANN last week was hacked and its DNS zone database
compromised. Attackers sent staff spoofed emails appearing to coming from icann.org. The organization said it was a "spear phishing" attack, and employees clicked on a link in the messages that took them to a bogus login page – into which staff typed their usernames and passwords, providing hackers with the keys to their work email accounts.

- Identified as a new strain of the ZeuS Trojan, Trojan-Banker.Win32.Chthonic, or Chthonic for short, is reported to have hit over 150 different banks and 20 payment systems in 15 countries. Financial institutions in the UK, Spain, the US, Russia, Japan and Italy appear to be the main targets of the malware. Exploiting computer functions such as web cameras and keyboards, Chthonic steals online banking credentials such as saved passwords.

- Researchers said more than 12 million devices running an embedded webserver called RomPager are vulnerable to a simple attack that could give a hacker man-in-the-middle position on traffic going to and from home routers from just about every leading manufacturer. Mostly ISP-owned residential gateways manufactured by some of the biggest names in the industry are currently exposed. The flaw, named Misfortune Cookie by the researchers who first discovered it, has been reported to all of the affected vendors and manufacturers, and most have responded that they will push new firmware and patches in short order.

**Legal, Litigation, Regulatory Risk**

- The National Credit Union Administration (NCUA) filed a lawsuit against a leading U.S bank over mortgage securities.

**Operational Risk**

- An article claimed that the two GSEs for housing are subsidizing homeowners by guaranteeing their mortgages and taking on greater risk. The article proposed to get the GSEs out of the business of refinancing home mortgages, claiming that by doing so would reduce the $5.3 trillion they currently guarantee and offer the private sector an attractive new market.

- An article reported that the Treasury Department decided to change the terms of the two GSEs’ conservatorships and sweep 100% of profits. The article claimed that this situation will prevent the GSEs from accumulating any cushion against future losses and potentially putting the taxpayers at further risk.

**Reputational Risk**

- A debt collector hired by a leading U.S. bank is accused of using threatening and racist language to intimidate customers into paying their debts.

- A leading U.S. bank failed to pass two of 31 tests designed to determine whether the bank is complying with a national mortgage settlement's rules. The tests involve sending pre-foreclosure letters to borrowers and notifications to people seeking mortgage modifications. The bank must implement a plan to "correct the behavior," and if it fails the tests on the same metrics again, it could face penalties.

- The Financial Industry Regulatory Authority (FINRA) fined a leading U.S. bank’s investment unit $1.9 million for "unfair pricing" related to the purchase of distressed securities over two years. The article highlighted that the regulator ordered the unit to pay more than $540,000 in restitution, plus interest, to affected customers.

- The Department of Treasury is seeking to order survival kits for all of its employees who oversee the federal banking system, according to a new solicitation. The emergency supplies would be for every employee at the Office of the Comptroller of the Currency (OCC), and delivered to every major bank in the United States. Contracts for survival kits are usually made for the military, or law enforcement such as the FBI.
Global Intelligence

China

- Sina Tech News reported that a worker strike broke out at a Liangwei Technology factory in Shenzhen’s Bao’an District, involving over a thousand people. The dissatisfied workers protested against reduced overtime pay and poor treatment from management. Liangwei Technology Company is based in Taiwan and mainly produces connectors, power cables, and other electronic components.

- Chinese news outlet reported that workers numbering a thousand have been on strike for the last 7 days at a leather goods factory in Shenzhen called Shenzhen Qingsheng Clothing and Accessories Limited Company. According to workers, the factory plans to relocate but the issue of wage and benefit arrears have not been resolved. The strikers have gained support from labor rights groups such as Hong Kong Confederation of Trade Unions and Students and Scholars Against Corporate Misbehaviour.

- Chinese news outlets reported that at Yili Anda (Guangzhou) Electronics Company, hundreds of workers who staged a sit-in protest over pay raises.

- Chinese news outlets reported that Intel has announced a new partnership agreement with Chinese online market JD.Com to expand cooperation in technological innovation of smart-hardware and development of user experience and enterprise-class products.

- China Labour Bulletin reported that Taiwanese touch screen manufacturer Wintek recently closed down two of its factories in Dongguan, Guangdong Province, dismissing 7000 workers. No labor protests were been reported.

- A Chinese news outlet reports a mutated version of Trojan_Mepaow.UEQ has been found. This malware are able to infect system’s cache directory create a new process to execute commands and automatically delete cache data.

- A page of QQ.com reports a trojan malware targeting Android devices dubbed as “Gathering trap” or “Party Trap” spreading via SMS messages. This malware is able to obtain user’s contacts and send out SMS messages phishing for other users to download a malicious application.

- A Chinese news outlet reports a security vulnerability on Android 4.3 or older version and found that some applications could obtain user information without user consent.

India

- On December 18, 2014 Business Standard reported Foxconn has informed its workers they do not have to come to the factory in Sriperumbudur, India for work from December 22, 2014 as the company was planning to suspend operations. According to the workers, the company so far has sent around 1,000 workers on leave with salary from a total 1,700 employees.

Malaysia

- A Malaysian news outlet reports the National Professors Council (MPN) proposed that the federal government amend the Employment (Amended) Act 2012 to cover the rights of foreign workers, as they are an important driver to the nation’s economy. This article is also shared by MTUC on its blog.

- A Malaysian news outlet reports dengue fever cases increased by 171.26% in Penang Island since January of this year.

- A Malaysian news outlet reports MEF proposed that the policies on employment for foreign workers needed to be changed.
A Malaysian news outlet reports MTUC’s statement regarding employees expectations of bonuses and salary increments are justified due to the increasing cost of living.

**North America**

- On December 16, 2014 Fox News reported that Qualcomm disclosed plans to lay off workers in San Diego within the next couple of months. The company filed a layoff notice on December 10 stating 178 of its San Diego workers will be let go by February. About 600 workers will be cut worldwide, including 300 in California, the newspaper reported.

**Vietnam**

- Lao Dong News reported that Ho Chi Minh City Ministry of Labor, Social Affairs, and Invalids issued a statement to the city's offices, organizations, and businesses to make sure they pay their employees' salaries and bonuses timely and provide employees with information regarding and when these payments will be given during this holiday season.

- Lao Dong News reported that on 12/16-12/17 nearly 400 workers from Eviron Company went on strike to protest against the way the company calculated employees' wages. According to workers, workers were hired and paid wages by the hour. People with higher skill sets were paid more but newly trained people had to work longer hours but were not compensated for the extra time spent. Company representatives stated that new employees did not produce enough unit/hour to warrant the extra money. Workers went on strike objecting the company’s calculation of wages based on units as oppose to hours spent.

**Legal and Regulations**

- The U.S. Department of Commerce’s Patent and Trademark Office (USPTO) will host its first Trade Secret Symposium on Thursday, January 8, 2015, at USPTO Headquarters in Alexandria, Virginia. The symposium will provide an opportunity for members of the public to hear from representatives of academia, government, legal practice and industry on important trade secret issues facing innovators today. Registration is available at [www.uspto.gov/ip/init_events/trade_secret_symposium.jsp](http://www.uspto.gov/ip/init_events/trade_secret_symposium.jsp). Attendees may also register at the door. Attendance is free. Further information about the symposium may be found in the Federal Register Notice.

- The National Labor Relations Board (NLRB or Board), in its December 11 Purple Communications, Inc. and Communications Workers of America, AFL–CIO decision, reversed certain Board precedent on employees' use of employers' email systems. The Board held that employees who have been given access to an employer’s email system in the course of their work are entitled to use the system to engage in statutorily protected discussions about their terms and conditions of employment while on nonworking time, absent a showing by the employer of special circumstances that justify specific restrictions.

- The National Institute of Standards and Technology (NIST) recently released an update on its Framework for Improving Critical Infrastructure Cybersecurity (The Framework). The Framework was first issued in February 2014 as a voluntary risk-based program to enable owners and operators of U.S. critical infrastructure to assess and remediate their cybersecurity risks. NIST welcomes ongoing feedback via email at cyberframework@nist.gov. It is soliciting input as to how organizations are using the Framework, and requesting specific suggestions for improvement and for possible outreach activities.
Pharmaceuticals

- In early November, the FBI and Europol announced ‘Operation Onymous’ – a joined-up international law enforcement action which saw the take-down of hundreds of dark markets on anonymous networks like Tor. These websites – which included Silk Road 2.0 - were selling illegal goods including weapons, drugs and hacker tools. However a report recently uncovered by SCMagazineUK.com sheds some doubt on how effective this action has been, with most darknet sellers, advertisers and buyers moving onto new – or undisturbed – market places.

- Pfizer is unlikely to come back with a fresh bid for AstraZeneca, chief executive Pascal Soriot told Swedish business daily Dagens Industri over the weekend.

- Several multi-national drug makers operating in Korea are adopting early retirement programs to cut jobs as part of a restructuring program amid sluggish sales, including Johnson & Johnson, Eli Lilly and Boehringer Ingelheim.

- China promised to speed up imports of drug and devices from the U.S. and enforce its anti-monopoly laws equally among Chinese and foreign companies.

- GlaxoSmithKline has refused to rule out cutbacks at its plant in Port Fairy, Australia, where painkillers are made, as part of a massive global restructure.

- Eleven new centres across England have been chosen to deliver the 100,000 Genomes Project. The 3-year project, launched by the Prime Minister earlier this year, aims to improve diagnosis and treatment for patients with cancer and rare diseases. The initiative involves collecting and decoding 100,000 human genomes - complete sets of people's genes - that will enable scientists and doctors to understand more about specific conditions.

- As according to Mc Kinsey report of India Pharma 2015 - Unlocking the Potential of the Indian Pharmaceutical Market, the Pharma industry has immense opportunities and has a projected market growth of USD 24 billion by 2015 and USD 55 billion by 2020.

- GlaxoSmithKline plc announced that its shareholders voted in "overwhelming majority" in favor of the company’s multi-billion swapping deal with Novartis AG in the annual shareholder meeting held on December 18.

- A leaked draft of the Trans Pacific Partnership trade agreement gives far too much intellectual property protection to brand drugmakers at the cost of generic competition, GPhA said Wednesday in a letter to the Obama administration.

- China’s FDA is threatening to severely punish companies that illegally manufacturer and sell codeine in the country, a warning the follows several revelations of the product was being sold in bulk quantities.

Retail

- Holiday shopping is up 15% from last year to $42.5 billion, according to a new comScore report. At least $1 billion of those figures came from online desktop sales. Additionally, retail cyber security remains a priority for companies in light of data breaches at Target, Home Depot, Neiman Marcus and others in the past couple years. Chief Information Security Officers (CISO) positions have become more common in retail companies’ senior leadership teams.

- The Pennsylvania Supreme Court ordered Wal-Mart to pay $188 million to employees who had sued the retailer for failing to compensate them for rest breaks and all hours
A security breach at Staples earlier this year may have exposed nearly 1.2 million customer payment cards. An investigation showed that the criminals used malware that may have allowed access to information for transactions at 115 of its U.S. stores, which total more than 1,400.

According to The Guardian, at approximately 7:00pm Friday night in London (1:00pm EST, 11:00am PST), Repricer Express--an automated service many third party Amazon sellers use to keep their prices competitive against each other--malfunctioned. Subsequently, it marked thousands of toys, clothes, cell phones, furniture and numerous other items for one penny, and many users dashed to cash out on the ultimate bargain sale.

Retailing Today reported that Walmart has announced the 75 winners of its Food Pantry Holiday Makeover campaign, which gifts a food pantry organization with a $20,000 grant for renovations. Over the past two weeks, communities nationwide came together to vote at walmart.com/holidaymakeover for their local food pantry to win a grant. The grants are being made to help the winning food pantries, such as the Chesapeake Cares Food Pantry in Huntingtown, Md., renovate their facilities and purchase essential equipment such as new refrigerators, ovens, stoves, storage units, and even refrigerated trucks to help them better serve families in need.

Kroger was announced the only grocery retailer to be granted elite Energy Star Certification status by the EPA. Elite status is conferred to organizations with at least 150 Energy Star rated buildings. Kroger has earned 649 Energy Star certifications.

Internet Retailer reported that PetSmart has agreed to be acquired by a consortium led by London-based BC Partners Inc. in a deal valued at $8.7 billion. Other members of the consortium include La Caisse de dépôt et placement du Québec, which manages public pension plans in the Canadian province of Quebec, and StepStone, a private equity firm based in New York.

On December 17, 2014 the Securities and Exchange Commission charged Avon Products, Inc., a global beauty products manufacturer and seller, with failing to put in place controls that could have detected and prevented payments made to Chinese government officials by employees and consultants at an Avon Chinese subsidiary from 2004 through the third quarter of 2008. In addition, Avon's books and records failed to accurately record the details and purpose of the payments. The SEC alleged that the conduct violated the Foreign Corrupt Practices Act. Avon has agreed to pay more than $67 million in disgorgement and prejudgment interest to settle the SEC's charges.

Parts of the Mall of America closed for part of Saturday afternoon due to an unauthorized demonstration by an estimated 1,500 protesters organized by Black Lives Matter.

A federal judge has ruled that customers suing Target for last year's data breach may move forward with their claims. U.S. District Judge Paul Magnuson in St. Paul, Minn., dismissed claims by plaintiffs in certain states but largely denied Target's request to toss out the proposed class action lawsuit. Magnuson rejected Target's argument that the consumers lacked standing to sue because they could not establish any injury.

On December 15, 2014 Amazon.com Inc. evacuated employees from its Seattle headquarters after a threatening note was spotted in a bathroom, according to local police.

A researcher has identified a stack buffer overflow vulnerability in Honeywell's OPOS (OLE for Retail Point-of-Sale) Suite, a solution that provides a standard programming interface for the integration of PoS hardware into retail PoS systems based on Microsoft Windows.
The rising intensity of POS threats has created a precarious environment for retailers looking to protect their customers' financial and personal data. POS systems are increasingly becoming a soft target for hackers, which is why it's more important than ever to consider the security of these machines and the information they store. There has been a resurgence of these attacks in the past few months, and the 2014 Verizon Data Breach investigation report listed them as a composition of top 9 breach vectors. The intrusions involve the attacker placing a special malware on the POS tills which captures payment card information while it is stored in the temporary memory.

Technology

- TechWeb China reported that several former Sony Mobile employees demonstrated with protest signs and banners outside of the company's mobile division headquarters in Beijing over layoffs which will allegedly impact 700-800 Sony Mobile (China) employees. Sony stated that the layoff plans have not been finalized and that they will make efforts to provide compensation and job transition assistance to laid off personnel.

- 2015 is expected to be the year of ransomware and attacks are likely to expand beyond consumers. Computers and mobile phones are not the only devices targeted by cybercriminals. As Internet of Things (IoT) devices become more popular, they will too make it on the crooks' list, especially since in many cases the manufacturer focuses more on the functionality of the product and less on securing it.

- The Chrome Security Team proposed that user agents (UAs) gradually change their user interfaces and experiences in order that they display non-secure origins as “affirmatively non-secure.” Google’s grand vision is that someday, HTTPS will become so widespread and commonplace that secure connections can be unmarked in the way that HTTP connections are currently.

- Counterfeit identities are the new hot product to support fraud new fake identity kits, passports, Social Security numbers, utility bills, and driver's licenses. A new identity, including a working SSN, name, and address

- Security researchers are making use of quantum physics to create fraud-proof credit cards, called Quantum-Secure Authentication (QSA). The technique centers on single particles of light, or photons, and their ability to encode data and exploits a property of photons that allows them to effectively be in multiple places at once.

- 2015 Security predictions include increased attacks in fileless payloads, rise in mobile malware, angler exploit kit will become the leading exploit kit, and a rise in the major internet of things attack will be observed.

- Qualcomm disclosed plans to lay off workers in San Diego within the next couple months. The company filed a layoff notice on December 10 stating 178 of its San Diego workers will be let go by February, the U-T San Diego reported Monday. Qualcomm said it was making changes as a way to be “more efficient.” About 600 workers will be cut worldwide, including 300 in California, the newspaper reported.

- A BBC documentary accuses Apple of breaking promises to improve working conditions at its suppliers, but Apple says it continues to make progress on a difficult issue.

- A strong U.S. dollar is terrific for American tourists on holiday trips abroad. But for U.S. software companies, the mighty greenback is a bummer.
Telecommunications

- The hacking attack on Sony Pictures may have been a practice run for North Korea’s elite cyber-army in a long-term goal of being able to cripple telecoms and energy grids in rival nations, defectors from the isolated state said.

Defense

- The experts from Kaspersky Lab’s Global Research and Analyst Team have compiled a list of top emerging threats in the APT world for 2015 which includes fragmentation of largest APT groups, targeting executives through hotel networks, enhanced evasion techniques, and new methods to exfiltrate data. APT groups will evolve to become stealthier and sneakier, in order to better avoid exposure.

- FBI has recently expanded its cybercrime team and moves cyber-threats to the top of law-enforcement’s agenda.

- The European Union on Friday filed a complaint at the World Trade Organization alleging that tax incentives provided by the state of Washington to Boeing Co. violated international trade rules.

Law Enforcement

- The FBI on Friday offered evidence that links the North Korean government to the hacking of Sony Pictures computers. Technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korean actors previously developed. There were similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks. The FBI also observed significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea, as well as several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack.

- According to John Pistole, the departing head of the TSA, terrorists remain stubbornly fixated on targeting airplanes and creating better bombs. Although it has been 13 years since a successful terrorist attack on Sept. 11, 2011 — terrorists seem committed to bombing a plane. “The threats continue,” Pistole, 58, said in an interview at the agency’s Arlington, VA, office. “They are persistent. The terrorists are innovative in their design, construction and concealment of devices.”

- Big-city police departments and union leaders around the country are warning the rank and file to wear bulletproof vests and avoid making inflammatory posts on social media in the days after a man ambushed two officers and shot them to death inside their patrol car. The slayings of Officers Rafael Ramos and Wenjian Liu on Saturday afternoon in Brooklyn heightened fears about the safety of law enforcement officials nationwide, though there is no evidence any threats are imminent. The gunman, 28-year-old Ismaaiyl Brinsley, had vowed in an Instagram post to put “wings on pigs” as retaliation for the slayings of black men at the hands of white police.
• A smartphone app that's under development will allow users to show the digital license to law enforcement officers during traffic stops and at security checkpoints at Iowa airports, according to Paul Trombino, director of the state Department of Transportation. The free app will be available sometime in 2015.

• Nordstrom has fired a sales associate who made a statement about killing police on his Facebook page. Aaron Hodges, 37, of Portland, suggested killing a white officer for every black man killed by police. His comment quickly circulated online, prompting complaints both online and directly to his employer.

• The Supreme Court ruled last week in an 8-1 decision that a police officer can stop a car based on a mistaken understanding of the law without violating the Fourth Amendment. The case arose from a traffic stop in North Carolina based on a broken brake light. But state law there required only a single working "stop lamp," which the car in question had. In an opinion by Chief Justice John G. Roberts Jr., the Supreme Court ruled that the officer's mistake was reasonable and so did not run afoul of the Fourth Amendment's ban on unreasonable searches and seizures.