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

Cyveillance provides educational webcasts on threat intelligence and other information security topics on a regular basis through our Cyber Intelligence channel on BrightTALK.com. Register now for our upcoming webinar series on 2015 trends in mobile, information, and physical security. Sign up today for one, two, or all three! February 24, 25, and 26.

Top Incidents

**Energy**

- American Association of Retired Persons (AARP) Ohio organized members residing in the FirstEnergy market to testify against a regulatory action that the Sierra Club has dubbed a “coal plant bailout.” There were three public hearings regarding the proposal last week, and AARP members testified at all three.

**Agribusiness**

- Legislation was passed on January 13, 2015 in the European Parliament allowing EU member states to restrict or ban GMO cultivation in their territories. This legislation goes into effect in the spring of 2015. Additionally, the law allows for nations to restrict or ban GMO's on a wide variety of grounds even though it may be allowed in the EU as a whole.
Insurance/Healthcare

- In yet another sign that medical device cybersecurity is becoming a growing concern, a new group has been formed to tackle the issue - the latest in a series of initiatives in this arena. The Health Information Trust Alliance, best known for its Common Security Framework, has launched a working group in an effort "to improve the overall security of and trust in health information technology, including systems and medical devices." The goal of the program "is to avoid, report and mitigate vulnerabilities related to health IT and medical devices."

Financial Services

- Due to a "technical malfunction" found in the computer systems of the Department of Defense, some federal retirees had their personal information sent to the wrong people. The compromised information included Social Security Numbers and tax statements.

Global Intelligence

- Japanese videogame giant Nintendo is hitting the pause button on operations in Brazil and will leave Latin America's largest market while it assesses how to deal with high import taxes. They are going to go back to the drawing board to create a totally new model in which pricing will "make sense" for their consumers. Setting up a local manufacturing base has not been viable and won’t be included in the plan.

Legal and Regulations

- On January 12, 2015, President Obama delivered a speech at the Federal Trade Commission during which he set forth several proposals, including the Personal Data Notification and Protection Act (the "Act"). The Act would institute a federal data breach reporting framework by requiring businesses that hold consumer data to issue alerts to those consumers within thirty days of a data breach.

Pharmaceuticals

- ‘Silk Road Reloaded,’ a new anonymous online drug market, draws upon a host of new anonymizing features, including I2P connectivity and the use of cryptocurrencies other than Bitcoin. By embracing I2P, the administrators of the new Silk Road iteration now welcome a service that, as opposed to Tor, is friendly to peer-to-peer connections and uses a design that is optimized for hidden services.

Retail

- Jewelry store robberies remain a persistent threat throughout the United States. Although the number of incidents nationwide has declined in the last year, some states along the East Coast have experienced a slight increase. The threat actors responsible for this increase are aggressive robbery crews that commit thefts from jewelry stores, primarily during business hours, and use similar methods and tactics. According to the Jeweler’s Security Alliance (JSA), the total number of jewelry crimes reported in 2013 decreased 8.1 percent, from 1,538 in 2012 to 1,414 in 2013; however, the total dollar loss from crimes against the jewelry industry in the United States increased 10.5 percent, from $60.2 million in 2012 to $66.5 million in 2013.1 The increase in monetary loss in 2013 is a result of an increase in the number of large, million-dollar robberies and burglaries.

Technology

- Popular messaging services like Snapchat and WhatsApp are in the cross hairs in Britain. That was the message delivered by Prime Minister David Cameron, who said he would pursue banning encrypted messaging services if Britain’s intelligence services were not given access to the communications.

Telecommunications

- It did not take long for the cable industry to speak out about President Barack Obama’s call to overturn state laws that prohibit the buildout of municipal-run broadband networks, with the presidents of the National Cable Telecommunications Association
Defense

- Systems that control the elevators, lights, ventilation, and fire alarms in federal buildings are vulnerable to cyberattacks that could compromise security or result in serious harm to government workers. In a report released within hours of high-profile social media hacks at U.S. Central Command, the Government Accountability Office said homeland security officials have little understanding of the risks presented by Internet-based control systems and don’t have a clear strategy for dealing with an attack if one were to occur.

Law Enforcement

- At least 50 U.S. law enforcement agencies have secretly equipped their officers with radar devices that allow them to effectively peer through the walls of houses to see whether anyone is inside, a practice raising new concerns about the extent of government surveillance. Those agencies, including the FBI and the U.S. Marshals Service, began deploying the radar systems more than two years ago with little notice to the courts and no public disclosure of when or how they would be used. The technology raises legal and privacy issues because the U.S. Supreme Court has said officers generally cannot use high-tech sensors to tell them about the inside of a person’s house without first obtaining a search warrant. The radars work like finely tuned motion detectors, using radio waves to zero in on movements as slight as human breathing from a distance of more than 50 feet. They can detect whether anyone is inside of a house, where they are, and whether they are moving.

Energy

- American Association of Retired Persons (AARP) Ohio organized members residing in the FirstEnergy market to testify against a regulatory action that the Sierra Club has dubbed a “coal plant bailout.” There were three public hearings regarding the proposal last week, and AARP members testified at all three.

- The Libyan branch of ISIS has claimed the abduction of 21 Egyptians.

- News article discusses how Sen. Bernie Sanders (I-VT) has forced Senate Republicans into a potentially embarrassing vote on whether or not climate change is real.

- The Gazette posts: Colorado has nearly 2,000 active oil and gas wells for every inspector and would need to add one inspector a year to keep up with recent trends, the state’s top energy industry regulator said Thursday. Oil and Gas Conservation Commission Director Matt Lepore provided the statistics in response to questions from Gov. John Hickenlooper’s task force on how the oil and gas industry is regulated. The panel was meeting in Greeley. Lepore said later that about 1,800 new wells have been drilled in Colorado every year over the past five to seven years, but falling oil prices could slow that rate and change the number of additional inspectors needed. Colorado has 1,959 active wells per inspector, a ratio that puts it in the middle of seven oil- and gas-producing states the commission surveyed. Alaska had the lowest ratio, about 370 wells per inspector. Wyoming had the highest, more than 2,900 wells per inspector. The average of the seven states was about 1,670 wells per inspector.

- Russia Today reports: A state-owned British train company that transports the nation’s nuclear waste is due to offer a passenger service along the Cumbria coast in northwest Britain, as demand for train travel rises and the UK’s railway network struggles to keep up. Direct Rail Services, a subsidiary of the Nuclear Decommissioning Authority, operates freight trains, and is expected to start passenger services next week, the Financial Times reports. The Department for Transport reportedly brokered the deal to prevent a crisis due to a shortage of trains in the north of England. The current diesel trains were to be exchanged for electric trains, but the electrification process has been slower than planned. Direct Rail Services will use two
locomotives that usually haul freight, including radioactive waste.

- Pennsylvanians Against Fracking have planned a rally at the Capitol Complex in Harrisburg to protest fracking during Governor Wolf inauguration ceremony. Environmentalists have sent email blasts asking for a “call to action” to help “disrupt” the ceremony. Sam Bernhardt, with Food & Water Watch, said the coalition expects to bring a couple hundred protesters to the rally. Josh Fox, director of anti-fracking documentary “Gasland,” is scheduled to attend the rally. The goal of the protesters, Bernhardt said, is to pressure Wolf into banning fracking, like Gov. Andrew Cuomo did in New York.

---

**Agribusiness**

- Trade officials from Japan and the United States opened a new round of talks in Tokyo on two sticking points, agriculture and automobiles, in negotiations for the 12-nation Trans-Pacific Partnership, said the Kyodo news service. The Foreign Ministry said it was unclear when the meeting would end. A U.S.-Japan agreement is viewed as essential to a TPP pact.

- Thurston County, Washington has become the first in Washington state to ban the use of neonicotinoid pesticides on government owned or managed land. This ban would cover about 2,700 acres of land around the county.

- Activist groups in Connecticut have been promoting their legislative goals for 2015 concerning GMO's. The deadline to file bills for the new legislative session was Friday, January 16, 2015. The post indicates that the group will be working to pass legislation banning the sale and use of GE grass seed and legislation which would remove the "trigger clause" from the Connecticut GMO Labeling Law passed in 2013.

- Legislation was passed on January 13, 2015 in the European Parliament allowing EU member states to restrict or ban GMO cultivation in their territories. This legislation goes into effect in the spring of 2015. Additionally, the law allows for nations to restrict or ban GMO's on a wide variety of grounds even though it may be allowed in the EU as a whole.

- On January 13, 2015, the European Parliament passed a directive allowing European nations to determine for themselves to allow, restrict, or ban genetically modified organisms. In response to this, the German Environment Ministry has called for a complete ban on GMO's in Germany. Additionally, the Green party in Germany has published an assessment warning that free trade agreements such as the TTIP and CETA could bring even more GMO's into European markets.

- The Arizona State House of Representatives is now considering the bill HB 2462 introduced by several representatives. The bill would require labeling of GMO's and would further ban the term "natural" from food labels if genetic modification was involved. The bill, which has been included in the supplemental section of this report, would take effect in June 2016.

- On January 15, 2015, the organization Circle of Blue posted via their Twitter account @circleofblue regarding the upcoming World Economic Forum. The tweet mentions water as one of the top issues of the Global Risk Report of this year's WEF. This could signal the topic gaining more traction with similar non-profit and activist organizations.

- Two leading farmers associations closed their accounts at Banco de la Nacion Argentina SA, the country's largest bank, to protest its refusal to extend financing to farmers holding on to their soybeans. The Argentine Rural Confederation, the country's largest rural NGO representing 109,000 farmers, decided at a members assembly to close its account, Ruben Ferrero, group president, said in an interview. Sociedad Rural will follow, saying the bank's only aim is to "harm the farmer by obliging him to sell up to the last bean," according to an e-mail statement.

- As discussed at the 96th annual American Farm Bureau Federation, agribusiness executives explored the future of technology in agriculture, food trends, and data
security. The public’s appetite for organic, GMO-free, gluten-free and locally sourced, sustainable foods will continue to grow, therefore educating the public about the science behind GMOs will become a priority. Other topics discussed include advancements in insect control, agronomic traits and soybeans in the future, and drought tolerance approaches.

- Food Business News reported that Krispy Kreme Doughnuts Inc. has developed a three-pronged expansion approach less than eight months after Anthony N. Thompson became President and CEO of the company. Thompson said he said Krispy Kreme will infill by expanding with existing franchise partners and growing out existing company-owned markets, which allows Krispy Kreme to leverage its supply chain efficiencies and capitalize on brand awareness.

- World Grain News reported that the Kellogg Co. is on the verge of acquiring an 85.93% stake in Bisco Misr, Cairo, Egypt, a maker of biscuits, cakes and wafers. The purchase price will be approximately $12.57 per share, for a total of $125 million.

- Food Production Daily reported that Ice River Springs, which makes plastic bottles and sells bottled water, was cited by the Occupational Safety and Health Administration (OSHA) and may incur penalties totaling $84,000 after an accident involving a packaging machine left a temporary worker permanently disabled.

- Mergers & Acquisitions News Today reported that The UK Government Competition and Markets Authority (CMA) has started an investigation after it found Sonoco’s acquisition of Weidenhammer Packaging Group gives rise to ‘a realistic prospect of a substantial lessening of competition’. Sonoco and Weidenhammer both manufacture and supply composite cans for food products such as gravy granules, chocolate powder, crisps, crackers.

- Tetra Pak’s press release reported that Finnish dairy producer, Valio, becomes the first company in the world to sell products to consumers in carton packaging made entirely from plant-based materials. Consumers are able to buy these packages at retail shops in Finland from this week.

- NJBiz reported that Popcorn maker Dale and Thomas Growers LLC is laying off 56 workers at its Englewood facility as the company alters its manufacturing arrangements. The company, which produces the Popcorn, Indiana, brand of snacks, will have about 100 employees left at the New Jersey facility after the layoffs, it said in a statement. It issued a WARN notice earlier this month that the workers would be laid off by March 27, 2015.

Insurance/Healthcare

- Health insurance companies in New Jersey will be required to protect client information by encrypting the data, under legislation Gov. Chris Christie signed into law recently.

- Healthcare organizations looking for help building an integrated approach to privacy and security compliance will soon have a new tool available. The Health Information Trust Alliance is adding privacy controls to the latest version of its Common Security Framework, slated to be released January 31, 2015.

- The Turkish Presidency’s State Audit Institution (DDK) recently revealed that the state failed to protect Turkish citizens’ ID information. It was determined in the course of the audit that the servers of the administration’s website had been breached and that ID information of citizens had been stolen. The perpetrators of the identity theft acquired medicine, prescription, and treatment information of the victimized citizens, who had no idea that their information had been stolen from the Social Security Administration.

- An investigation by The Toronto Star has revealed that thousands of serious health-related privacy violations go unreported each year to the provincial Information and Privacy Commissioner. Nearly all of the 218 privacy breaches uncovered in documents obtained by the Star — which occurred at just eight of Toronto’s biggest health
institutions — were not reported because of a legislative loophole that allows hospitals to handle such violations internally.

- When the Star provided some examples of unreported cases to acting privacy commissioner Brian Beamish, he called for a legislative change to force hospitals to report serious breaches of personal health information.

- In a speech at the Federal Trade Commission on January 12, 2015, President Obama proposed a nationwide breach notification standard that would require all U.S. companies to notify consumers of a breach within 30 days.

- A federal advisory panel has kicked off discussions about the privacy and security challenges related to the use of big data in healthcare, with a goal of making policy recommendations in the coming weeks.

- In yet another sign that medical device cybersecurity is becoming a growing concern, a new group has been formed to tackle the issue - the latest in a series of initiatives in this arena. The Health Information Trust Alliance, best known for its Common Security Framework, has launched a working group in an effort “to improve the overall security of and trust in health information technology, including systems and medical devices.” The goal of the program “is to avoid, report and mitigate vulnerabilities related to health IT and medical devices.”

---

**Financial**

**Financial Services**

**Activism**

- Global fossil fuel divestment actions will occur on February 13-14, 2015 in the London, UK financial center. The actions are expected to be well attended by protesters.

- Protests will occur outside the World Economic Forum in Davos, Switzerland from January 21-24, 2015. Participants will demand equal rights for the middle class as well as environmental protection policies.

- OWS activists held several anti-Wall Street protest events in New York City on Dr. Martin Luther King Jr. Day, January 19, 2015

- Unions representing bank employees in Italy said January 12, 2015 they will go on strike on January 30, 2015 due to worker rights disagreements. The general strike would involve several unions and labor federations that have already announced plans to hold large-scale organized events in Milan, Rome, Ravenna and Palermo to show their support for the strike.

**Information Security Risk**

- A hacker group leaked details of about 30,000 clients of a small Swiss bank, after the bank declined the group’s request to pay a ransom. The hackers’ asking price for continued privacy was 10,000 euros.

- Researchers discovered a new strain of the Vawtrak banking Trojan that’s delivered by malware downloader called Chanitor. Vawtrak is also known as Neverquest and Snifula. Once the malware infects a machine, the threat injects the web browser process with a DLL that can direct the infected browser to specific destinations that have already been compromised. When the victim’s browser loads the compromised page, the malware injects code in real time, adding content designed to trick the user into providing sensitive information, such as banking credentials, which are then transmitted to a remote machine controlled by cybercriminals.

- A leading ICS/SCADA security researcher warned that traditional banking Trojan malwares posing as legitimate ICS software updates and files are targeting plant floor networks rather than nation-state custom malwares in the wake of Stuxnet, an infamous computer worm that reportedly compromised Iranian PLCs, collecting
information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart. Attacks appear to be coming from traditional cybercriminals rather than nation-state attackers, and are not using cyber espionage-type malware. The researcher said these traditional cybercriminals are looking for targets in the ICS/SCADA world because they are looking for revenue rather than spying or sabotage purposes.

- New research shows that complacency and low levels of security awareness are contributing to a major insider threat facing UK organizations today. The research found that just over half (58%) were aware of security threats and the risks they pose to corporate information while 39% said they thought it was the company’s responsibility to protect data. More worryingly, almost two-thirds (62%) said they thought their behavior only has a low to moderate impact on security and nearly a half (48%) claimed they weren’t bothered about their corporate security policy as it didn’t affect their role. Interestingly, twice as many said they were more careful about data security at home (24%) than at work (12%).

- Researchers discovered a new malware dubbed “Skeleton Key” that can evade IDSs that monitor both software and abnormal user behavior. The malware can bypass Active Directory systems that only use single-factor authentication. Researchers explained that Skeleton Key is deployed as an in-memory patch on a victim’s AD domain controllers to allow the threat actor to authenticate as any user, while legitimate users can continue to authenticate as normal.

- Experts are calling on Google to rethink its patch priorities after it confirmed that it will no longer update a critical component that runs on Android 4.3 “Jelly Bean” and older devices. As a result, 83 percent of all Android smart phones and tablets - or about 930 million devices - will be running a version of Android that contains known vulnerabilities that an attacker could remotely exploit to seize control of the device or steal the data it stores.

- Researchers warned that a new user-friendly attack toolkit is currently on the market, and it's being actively used by Brazilian banking fraudsters. It features a user-friendly interface that includes a "start phishing" button. And it effectively circumvents both two-factor authentication and device identification protections. The kit is called KL-Remote, a remote overlay toolkit that performs what it calls "virtual mugging." Unlike banking Trojans, KL-Remote is less automated. It requires attackers to do some manual sleight of hand, but it makes it very easy to pull off. The toolkit is distributed by being embedded in other malware. It comes preloaded with a list of targeted banking URLs. When the infected user visits one of those sites, the malware operator gets an alert and can then decide whether or not to proceed with an attack.

- A Texas-based hotel management company began notifying an undisclosed number of individuals that malware was found on three point-of-sale (POS) terminals used at food and beverage outlets in one of their hostels in California, and that their payment card information may have been compromised. The POS system was compromised from July 26, 2014, to September 2, 2014.

- The website of a Tennessee-based pet supply store began notifying several thousand customers that unauthorized individuals accessed its servers and installed malicious files to capture personal information – including payment card data – entered into its website. The store said the malicious files have been removed, and additional steps have been taken to secure the system against future breaches. The breach is believed to have occurred from November 25, 2014, to December 29, 2014.

- Due to a “technical malfunction” found in the computer systems of the Department of Defense, some federal retirees had their personal information sent to the wrong people. The compromised information included Social Security Numbers and tax statements.

**Legal, Litigation, Regulatory Risk**

- A leading U.S. financial services company is challenging the federal government's decision to subject the insurer to stricter oversight, setting up the biggest test yet for regulators responsible for protecting the U.S. financial system from another crisis. The lawsuit pits the nation’s largest life insurer by assets against the Financial Stability
Oversight Council, a group of top financial regulators created by Dodd-Frank and given authority to identify companies that could threaten the U.S. economy in a crisis. The financial firm, which is the fourth nonbank to be designated as “systemically important” by the council, is the first company to legally challenge that conclusion. The label means that the insurance provider could pose significant risks to the U.S. financial system should it collapse and warrants tougher oversight, which could crimp its ability to raise dividends and buy back shares.

- A Miami, Florida-based law firm paid $250,000 to settle a lawsuit filed by the Federal Deposit Insurance Corp. alleging negligence in the law firm's handling of a real estate loan by its client, a failed bank based in Englewood, FL.

- The U.S. Supreme Court on January 12, 2015 declined to hear an appeal filed by several banks objecting to a lawsuit filed by a federal regulatory agency over their alleged role in selling mortgage-backed securities to now-failed credit unions.

- The House passed a bill January 14, 2015 that alters sections of the 2010 Dodd-Frank financial overhaul. Most notably, the measure passed would give U.S. banks two extra years - until 2019 - to ensure that their holdings of certain complex and risky securities don't put them out of compliance with a new banking rule.

- The U.S. Supreme Court handed a win to mortgage borrowers when they unanimously ruled a lender erred when it insisted that borrowers who opted to back out of a mortgage because of disclosure errors by the bank had to go to court to do so. Instead, the Court said a mere letter to the bank was sufficient notice under the Truth in Lending Act so long as it was within the three-year window the Act allows.

- U.S. regulators ordered a Swiss global financial services company to pay more than $14 million in penalties for a series of rule violations from 2008 to 2012 at its internal venue for trading stocks. The investment bank was cited by the Securities and Exchange Commission for letting users of its dark pool submit orders at prices denominated in increments smaller than a penny, something SEC rules prohibit because it can be used to get a better place in line when buying or selling stock.

**Operational Risk**

- The Russian Central Bank said a leading U.S. credit card payment company and Russia’s National System of Payment Cards (NSPC) agreed on providing operational services and payment clearing services for domestic transactions through the NSPC processing center. The two entities signed the agreement on December 30, 2014, according to a press release. The move will grant the U.S. payment service company a remission of paying the security deposit to the Central Bank.

- New York's top law enforcement official said he plans to help bring more fraud cases against the world's biggest banks for selling shoddy mortgage-backed securities before the 2008 financial crisis. The state’s attorney general said some of these banks were involved in the same kind of wrongdoing that has led him since 2012 to join the federal government in multi-billion-dollar cases against the three-largest U.S. banks. The attorney general said there were many more institutions involved, and therefore there will be more cases.

**Reputational Risk**

- A leading Scottish bank admitted to mis-selling loans to business customers under a taxpayer-backed program. The bank has loaned more than £900 million to 9,000 small firms since the Enterprise Finance Guarantee (EFG) was set up in 2009 to help businesses who would otherwise find it difficult to access credit. It is the biggest user of the program. But following reported complaints from small firms and discussions with an economic development bank owned by the UK Government, which is overseeing the program, it reviewed a sample of EFG customer files. The Scottish bank, which is 80% owned by the Treasury, said the review identified a number of instances where they have not properly explained to customers how borrower and guarantor liabilities work under the EFG program.

- A mutual fund billionaire is accused of helping defraud the heir of one of the earliest investors of his mutual fund company out of $150 million. The legendary businessman
built the publicly traded mutual fund business into a juggernaut that has nearly $900 billion under management and a market value of about $34 billion. He is also a highly respected philanthropist, recently pledging $250 million to an Ivy League university, his alma mater.

Global Intelligence

Brazil

- The ex-Chief of International Operations of Petrobras, Nestor Cerveró, was arrested and denied bail in the ongoing corruption investigation. The investigation has the potential to eventually reach President Dilma, a former Petrobras board member and whose political party was the main beneficiary of the state run company's kickback scheme. Investigators said this week the total amount of money involved could exceed $28 billion, making it Brazil's biggest-ever money laundering probe. Police are also investigating the possible involvement of more foreign companies and 750 infrastructure projects in addition to the contracts involving Petrobras.

- Japanese video game giant Nintendo is hitting the pause button on operations in Brazil and will leave Latin America's largest market while it assesses how to deal with high import taxes. They are going to go back to the drawing board to create a totally new model in which pricing will "make sense" for their consumers. Setting up a local manufacturing base has not been viable and won't be included in the plan.

- Brazil's GDP has fallen 1% in relation to the $2.25 trillion in the first three quarters of 2014 due to the decline of exports of raw materials. California's data on the other hand has expanded in 2014 in almost every metric from the $2.20 trillion they hit in 2013.

- Arrest warrants for 15 drug traffickers in the Santa Teresa slums in Rio de Janeiro were issued after the criminals exposed their exploits, weapons, and peers in Facebook photos and postings urging further attacks on the local police.

- Fans can now register online for Olympic ticket sales that will begin in March for the August 2016 games, the first ever in Latin America. Brazil is reserving 70% of the tickets for Brazilians. A total of 7.5 million tickets will be offered, more than half at $27 or less. Preparations for the Rio Olympics are running behind schedule and over-budget, but the organizers say all the venues and infrastructure projects - including a new subway line - will be ready for the Games.

China

- An article on QQ.com reports that due to the approaching Lunar New Year, many Internet users are using a "ticket grabbing" application to purchase transportation tickets for going home on the holiday. Some criminals are exploiting this trend and bundling dubbed as "Pinocchio" into the these applications. According to the article, this malware could infect computers as well as mobile devices.

- Chinanews.com reports Tencent QQ Mobile Devices Managers detected several types of malware injected into the Whatsapp application. The compromised version of the app is being spread through mobile device forums and mobile app stores.

- Several users on WooYun.org reports multiple security vulnerability attributes to China Mobile. This could be a security threat to HP as some HP China employees could be using China Mobile as their telecommunication provider.

- An article on Xinhuanet.net reports a SMS fraud being used to scam users' banking information. According to the article, a user received an SMS from "10086" which is associated with a major Chinese major telecommunication service provider, China Mobile, requesting banking information for claiming accumulated reward points. The user replied to the counterfeit "10086" number and later found that 52,000RMB were transferred out of his bank account. Later, an investigation found that the SMS from 10086 was embedded with Trojan malware.
A Chinese technology website reports hackers using Pastebin as a hosting server for backdoor malware and directly loading malware from Pastebin instead of hackers’ servers.

A posting on It165.net reports Asus routers contained a remote command execution vulnerability that affected all versions of firmware.

A Chinese technology website reports a security vulnerability on Mac OS X Spotlight that could expose IP, email addresses and other information.

A posting on Jifang360.com reports eight security vulnerabilities affecting version 1.0.0 and 1.0.1. According to the article, two vulnerabilities that pose the most threat among the eight have been ranked moderate-security threat. One of the moderate-security vulnerabilities could be used to launch DDoS attacks, the other could lead to memory leaks caused by dtls1_buffer_record being used in certain conditions.

A Chinese media source reported that a major protest broke out at an HP subsidiary in China after thousands of employees refused to accept HP’s China head as their new chairman on January 19, 2015. Employees at H3C Technologies Co. Ltd., a Hangzhou-based communications equipment maker purchased by HP in 2010, said the new appointment, which was not made official until Monday afternoon, will endanger the company's autonomy in operation. About 2,800 employees in Beijing and Hangzhou have signed a petition against the unconfirmed appointment, according to the organizers of the protest. H3C has around 4,800 employees, Beijing is the base of its marketing while Hangzhou mainly heads development.

Europe

The EU Commission’s websites are again available for TOR users. TOR users are not blocked any longer from access to the resources. Restrictions were put in place in 2012, meant to safeguard the pages against cyber-attacks. However, laws in at least some of the EU member states prohibit discrimination against anonymous web users.

Japan

The Japan Times reported that labor unions at major electronics makers are planning to demand a hike of ¥6,000 in monthly pay across the board during the upcoming “shunto” annual pay negotiations, industry sources say. It would be the highest demand since a ¥7,000 request filed in 1998. The unions at 13 major manufacturers, including Hitachi Ltd., Toshiba Corp. and Mitsubishi Electric Corp., usually unify their demands ahead of such negotiations. It refers to the annual wage negotiations between the enterprise unions and the employers. Many thousands of these unions conduct the negotiations simultaneously from the beginning of March.

Malaysia

In a posting on Good Electronics reports The Electronic Industry Citizenship Coalition (EICC), a nonprofit coalition of leading electronics companies dedicated to supply chain responsibility, announced that it will conduct shadow audits and increase its industry and government engagement in Malaysia to further combat forced labor.

North America

Gizmodo reported that somebody hacked the Lizard Squad’s DDoS-for-hire service last week. According to the article, the hacker group left all their customers’ data in plain text and $11,000 in bitcoin in the open.

Hankyoreh reported that despite serious conditions among victims, Samsung says they’ll only compensate employees with particular illnesses. Samsung’s compensation plan stated that Samsung would only compensate people with breast cancer, brain tumors, and five kinds of blood cancers including leukemia. Samsung said that it would only compensate people who had worked at least one year in the case of blood cancers and at least five years in the case of brain cancer and breast cancer.

Tech Crunch reported that Apple is sending out notices of termination to people whose accounts are registered in Crimea, citing sanctions that the U.S. has ordered against
the region as a response to Russia annexing it earlier in 2014. This means the developers cannot create nor publish apps in Apple's App Store.

- A media source reported that four of the world’s largest tech giants, Apple, Google, Intel, and Adobe, have agreed to a new settlement of 4415 million in an attempt to resolve a lawsuit that alleges the firms had a no-poaching agreement. The lawsuit claimed that the agreement prevented workers from getting better job offers elsewhere. The 2011 case claimed $3 billion in damages on behalf of more than 64,000 workers at the four firms.

Legal and Regulations

- On January 12, 2015, President Obama delivered a speech at the Federal Trade Commission during which he set forth several proposals, including the Personal Data Notification and Protection Act (the “Act”). The Act would institute a federal data breach reporting framework by requiring businesses that hold consumer data to issue alerts to those consumers within thirty days of a data breach.

- On January 13, 2015, President Obama visited the National Cybersecurity and Communications Integration Center to announce a variety of legislative and administrative proposals, many of which were updates to his 2011 Cybersecurity Legislative Proposal, designed to confront Cybersecurity threats. In addition, the President announced a White House Summit on Cybersecurity and Consumer Protection, to be held at Stanford University on February 13, 2015.

- On the heels of President Obama’s proposal to create a national data breach notification standard, yesterday, New York Attorney General, Eric Schneiderman announced that he will propose legislation that would significantly strengthen New York’s existing data security laws and establish new consumer privacy protections. For more information on the current state data breach notification statutes: http://www.dwt.com/statedatabreachstatutes/.

Healthcare

- New legislation signed by New Jersey Governor Chris Christie late last week mandates that health insurance companies in the state protect the personal information they compile or maintain through encryption or “by any other method or technology rendering it unreadable, undecipherable, or otherwise unusable by an unauthorized person.”

Financial Services

- Adding to the banks’ compliance obligations, effective immediately, banks chartered or licensed in New York will now face an updated Cybersecurity examination process, Superintendent of the Department of Financial Services (DFS) Benjamin M. Lawsky announced in a memorandum. Additions to regulatory examinations will cover areas ranging from protections against intrusion and the configuration of servers and databases to the organization and reporting structure for cyber security issues. To read Superintendent Lawsky’s memorandum, click here.

Pharmaceuticals

- Federal authorities arrested five people in connection with a “pill mill” that allegedly sold narcotics prescriptions at an L.A. clinic and supplied illegally-obtained prescription drugs to Texas. The five, including the operator of a now-shuttered Harvard Heights clinic and a doctor who worked there, were charged in a grand jury indictment last week with narcotics trafficking and selling prescriptions for potent and addictive painkillers, anti-anxiety medication and cough syrup that are popular among addicts.

- Health insurance companies in New Jersey will be required to protect client
information by encrypting the data, under legislation Gov. Chris Christie signed into law. The bill follows a series of incidents involving stolen laptops containing policyholder information protected only by user passwords.

- ‘Silk Road Reloaded,’ a new anonymous online drug market, draws upon a host of new anonymizing features, including I2P connectivity and the use of cryptocurrencies other than Bitcoin. By embracing I2P, the administrators of the new Silk Road iteration now welcome a service that, as opposed to Tor, is friendly to peer-to-peer connections and uses a design that is optimized for hidden services.

- Pfizer informed New York State labor officials that it will lay off 50 workers at its Pearl River plant by April, reported Lohud. The company indicated that it has 1330 total employees at the facility, the same figure cited last year when it told the state it would lay off 44 workers around June 17, 2014.

- Johnson & Johnson said in a court filing on Wednesday that women are being illegally solicited by unknown callers trying to persuade them to sue over transvaginal mesh devices, which are the subject of more than 35,000 lawsuits against its Ethicon Inc subsidiary.

Retail

- Jewelry store robberies remain a persistent threat throughout the United States. Although the number of incidents nationwide has declined in the last year, some states along the East Coast have experienced a slight increase. The threat actors responsible for this increase are aggressive robbery crews that commit thefts from jewelry stores, primarily during business hours, and use similar methods and tactics. According to the Jeweler’s Security Alliance (JSA), the total number of jewelry crimes reported in 2013 decreased 8.1 percent, from 1,538 in 2012 to 1,414 in 2013; however, the total dollar loss from crimes against the jewelry industry in the United States increased 10.5 percent, from $60.2 million in 2012 to $66.5 million in 2013.1 The increase in monetary loss in 2013 is a result of an increase in the number of large, million-dollar robberies and burglaries.

- After close to two years of meager sales and no hope for turning a profit for at least another six years, Target Canada has decided to suspend all its operations in Canada. The company announced Thursday it would cut its losses in Canada, file for creditor protection, and shutter all 133 Target Canada stores after 22 months of multi-million dollar losses.

- The Wet Seal Inc., a teen clothing retailer, has filed for Chapter 11 bankruptcy protection. The announcement Friday comes a little over a week after the chain said that it was closing 338 stores, or about two-thirds of its total store count.

- Retailers looking to replenish inventories depleted by solid holiday sales are facing a new impediment at West Coast ports. Reuters is reporting that unions are orchestrating work slowdowns to exacerbate an already gridlocked situation at the busy port. The Pacific Maritime Association said the region’s five largest ports, including Los Angeles and Long Beach, had seen backups “approaching complete gridlock,” as contentious contract talks with the dockworkers union have stalled.

- Online retail continues to compete with in-store sales. Jet and Boxed are two online retailers taking aim at the warehouse club channel. Both have a long ways to go to rival the volume of Sam’s Club and Costco but are increasingly on their radar. Online grocery shopping is growing and Amazon’s pricing strategy is competitive with Walmart’s.

- CNet reported that Apple Inc. plans to open five new stores across China over the coming five weeks before the Chinese New Year on February 19, 2015. Apple currently has 15 stores open in the country.

- Retailing Today reported that the Toys “R” Us annual fundraising campaign to benefit the Marine Toys for Tots Foundation was its most successful to date, raising $6.4
million and collecting more than 220,000 toys. At Ikea, millions of customers and employees around the world participated in the IKEA Soft Toys for Education campaign, which raised $12 million for UNICEF and Save the Children educational projects.

- The Minneapolis Star Tribune reported that after racking up $2 billion in losses by the end of 2013, Target Corp. announced that it will shutter 133 stores in Canada and will instead focus its energies on revitalizing its core 1,800-store U.S. business.

- CNN Money reported that RadioShack is allegedly preparing to file for bankruptcy as soon as next month. The company was struggling with $841 million in long-term debt as of its most recent financial statement. Additionally, RadioShack had previously disclosed it needed $100 million in combined cash and available credit by Jan. 15. Without that, its major creditors could pull the plug on the long-term financing it needs to survive. Currently, the company is in talks to sell leases to Sprint Corp.

- Bloomberg reported that states could collect sales taxes on out-of-state purchases made over the Internet, in a draft proposal being circulated by U.S. House Republican, Representative Bob Goodlatte of Virginia. The proposal differs from a plan that passed the Senate in 2013 with the support of major retailers including Amazon.com Inc. and Wal-Mart Stores Inc. Amazon.com is No. 1 in the Internet Retailer Top 500; Walmart.com is No. 4.

- ABC News reported that Chipotle has stopped serving pork at hundreds of its restaurants after suspending a supplier that violated its standards. Chris Arnold, a spokesperson for the Mexican food chain said most of the issues related to the violations concerned the housing for the pigs. Chipotle demands that its suppliers raise pigs in humane conditions with access to the outdoors, rather than in cramped pens.

- Amazon’s tax arrangements in Luxembourg may give the U.S. online retailer an illegal advantage over competitors, European Union regulators said Friday. At issue are the prices that multinational companies charge for goods or services sold by one subsidiary to another, known as transfer-pricing arrangements.

Technology

- Popular messaging services like Snapchat and WhatsApp are in the cross hairs in Britain. That was the message delivered by Prime Minister David Cameron, who said he would pursue banning encrypted messaging services if Britain’s intelligence services were not given access to the communications.

- BrandChannel reported that IBM and Apple announced a partnership back in July to create a suite of apps for mobile devices and the enterprise B2B market. The latest sector the global brands are teaming up to improve: retail, with two new apps for retailers revealed today at America's National Retail Federation annual conference, aka the NRF Big Show 2015, in New York.

Telecommunications

- It did not take long for the cable industry to speak out about President Barack Obama’s call to overturn state laws that prohibit the build out of municipal-run broadband networks, with the presidents of the National Cable Telecommunications Association (NCTA) and American Cable Association (ACA) issuing statements about how they think overturning such laws will cause damage.

- Sprint said that it wouldn’t object if regulators reclassified the Internet as a utility, breaking from the position of most major Internet providers in the country.

- Google is apparently close to investing in rocket maker SpaceX, creating a formidable alliance in Silicon Valley’s accelerating Internet space race. The goal is to support the
development of SpaceX satellites that could beam low-cost Internet around the globe to billions who don’t have it.

Defense

- On January 12, 2015, the hacking group CyberCaliphate accessed the Twitter and YouTube accounts of U.S. Central Command (CENTCOM). Tweets were sent by CyberCaliphate from the CENTCOM Twitter account. On January 12, 2015, at 2:01PM CST, @TheAnonMessage, a Twitter account associated with the Anonymous hacking group, tweeted 11 IP addresses involved with the CENTCOM hack with the message, “We’ve traced the hacker who infiltrated @CENTCOM to somewhere in the state of Maryland. @FBI, you’re welcome.”

- Systems that control the elevators, lights, ventilation, and fire alarms in federal buildings are vulnerable to cyberattacks that could compromise security or result in serious harm to government workers. In a report released within hours of high-profile social media hacks at U.S. Central Command, the Government Accountability Office said homeland security officials have little understanding of the risks presented by Internet-based control systems and don’t have a clear strategy for dealing with an attack if one were to occur.

- The day before Islamic radicals hijacked Central Command’s Twitter account, the Defense Information Systems Agency officially launched a major overhaul intended, among other things, to increase cybersecurity. But it doesn’t mean the office is getting bigger or getting more money: DISA’s cybersecurity office will actually get smaller.

- The Defense Information Systems Agency (DISA) released new cloud security guidance Tuesday, effectively codifying how Defense Department agencies will use commercial cloud products.

- The US and UK will immediately begin work on a series of large scale joint exercises to test the resilience of each other’s online infrastructure, according to the U.K. government.

Law Enforcement

- At least 50 U.S. law enforcement agencies have secretly equipped their officers with radar devices that allow them to effectively peer through the walls of houses to see whether anyone is inside, a practice raising new concerns about the extent of government surveillance. Those agencies, including the FBI and the U.S. Marshals Service, began deploying the radar systems more than two years ago with little notice to the courts and no public disclosure of when or how they would be used. The technology raises legal and privacy issues because the U.S. Supreme Court has said officers generally cannot use high-tech sensors to tell them about the inside of a person’s house without first obtaining a search warrant. The radars work like finely tuned motion detectors, using radio waves to zero in on movements as slight as human breathing from a distance of more than 50 feet. They can detect whether anyone is inside of a house, where they are and whether they are moving.

- The FBI is increasing its arsenal against international corruption by creating three squads tasked with rooting out bribery cases that happen overseas but have repercussions for the U.S., the Associated Press report. Corruption in foreign countries is becoming a bigger focus of the FBI’s because of the expansion of the global economy, where corruption can have a rippling effect. The initiative calls for sending about 30 agents to squads based in New York, Washington and Los Angeles. The mission of the three squads is to enforce the Foreign Corrupt Practices Act, which bars the bribery of foreign government officials.
Activists protesting what they call "police and state violence against black people" chained themselves to concrete-filled barrels and blocked a busy Boston-area highway at the height of the Thursday morning commute. State police shut down northbound Interstate 93 south of the city, and I-93 south, in Medford, north of the city, at about 7:30 a.m., inconveniencing thousands of drivers and causing miles-long backups. The southbound lanes were reopened at about 8 a.m. and the northbound lanes at about 10 a.m. after police and firefighters used power saws to cut protesters out of the barrels to which they were attached while lying in the roadway.