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
- Technology
- Telecommunications
- Entertainment
- Defense
- Law Enforcement

2015 Security Trends Webinars

Join us in February for a three-part webinar series on mobile, information, and physical security trends.

Dates:
February 24, 25, & 26

Time:
10:00AM PT | 1:00 PM ET

Top Incidents

Energy

- The United Steelworkers union, which represents employees at more than 200 U.S. oil refineries, terminals, pipelines and chemical plants, began a strike at nine sites on Sunday, the biggest walkout called since 1980. The USW started the work stoppage after failing to reach agreement on a labor contract that expired Sunday, saying in a statement that it “had no choice.” The union rejected five contract offers made by Royal Dutch Shell Plc on behalf of oil companies including Exxon Mobil Corp. and
Chevron Corp. since negotiations began on January 21. “The problem is that oil companies are too greedy to make a positive change in the workplace,” USW International Vice President Tom Conway said in the statement. “They continue to value production and profit over health and safety, workers and the community.”

**Agribusiness**

- Five environmental, animal welfare and community organizations filed suit in federal district court in Washington, DC, to force EPA to set air pollution standards for large livestock farms. The lawsuit asks the court to order EPA to act on a 2009 petition by the groups asking for the standards. “This failure to act is particularly egregious given the extreme risk to human health and welfare and the environment caused by aerial pollutants originating from CAFOs (confined animal feeding operations),” say the groups, the Humane Society of the United States, Association of Irritated Residents, Environmental Integrity Project, Friends of the Earth and the Sierra Club.

**Insurance/Healthcare**

- Federal regulators have unveiled a draft roadmap for achieving nationwide secure health data exchange built on interoperable electronic health records systems within the next three years.

**Financial Services**

- A Dutch judge ruled that an accused Russian “sophisticated hacker” can be extradited to the United States. The suspect, along with four other accomplices, four Russians and a Ukrainian, are accused of stealing credit and debit card numbers and other personal information from well-known U.S. companies and selling them online. Just three of the corporate victims have reported combined losses in excess of $300 million. The online theft case is reported to be one of the largest US corporate hacks of more than 160 million credit card details.

**Global Intelligence**

- Over ten different activist groups are uniting their efforts to have a large protest against political corruption at the congressional building in Brasilia. Lawmakers all return Sunday to be sworn in and elect their congressional leaders. Protesters plan to be there from 8 a.m. bussed in from five different states, with over 300 banners protesting corruption and calling for the impeachment of President Dilma.

**Legal and Regulations**

- A committee established by Google is review whether the decision by the European Court of Justice to enforce the “Right to Be Forgotten” on the internet be imposed beyond Europe’s shores? New York Times reports.

**Pharmaceuticals**

- Pfizer has reached an agreement in principle to pay $400 million to settle a class-action securities lawsuit that alleged the drug maker illegally marketed several medicines and, subsequently, caused investors to lose money, according to a filing with the U.S. Securities and Exchange Commission. The lawsuit alleged that, between January 2006 and January 2009, Pfizer marketed several drugs on an off-label basis.

**Technology**

- US business groups are seeking “urgent discussions” over new Chinese rules requiring foreign firms to hand over source code and other measures. The groups wrote to senior government officials after the introduction of the cybersecurity regulations at the end of last year. The US Chamber of Commerce and other groups called the rules “intrusive”. The regulations initially apply to firms selling products to Chinese banks but are part of a wider review. “An overly broad, opaque, discriminatory approach to cybersecurity policy that restricts global internet and ICT products and services would ultimately isolate Chinese ICT firms from the global marketplace and
weaken cybersecurity, thereby harming China’s economic growth and development and restricting customer choice,” the letter read.

**Telecommunications**

- Verizon agreed to a $5 million settlement after admitting that it failed to investigate whether its rural customers were able to receive long distance and wireless phone calls. The settlement is part of the Federal Communications Commission's attempt to fix the rural call completion problem, which extends beyond just Verizon's network.

**Entertainment**

- Prior to the New England Patriots facing the Seattle Seahawks in Super Bowl XLIX, researchers warned that at least one of the official National Football League (NFL) mobile applications is plagued by serious vulnerabilities that expose users' personal information. According to Wandera, a company that provides mobile data gateway solutions for enterprises, the official NFL Mobile apps for iOS and Android are vulnerable to man-in-the-middle (MitM) attacks.

**Defense**

- Amid reports of Australia deploying cyber weapons in the Middle East in a counter-terrorism operation, a cyber-espionage program was discovered being used by several countries in sophisticated hacking operations. Security experts revealed the existence of the spying software after former NSA contractor Edward Snowden allegedly leaked the source code.

**Law Enforcement**

- A license plate tracking program established to seize cars and money to combat drug trafficking has gone far beyond its original scope and has led to the collection and storage of millions of records about motorists, Reuters reports. Not only is the database being used to track drug dealers, but state and locals authorities are using it to search for cars tied to other serious crimes, raising questions among privacy advocates.

**Energy**

- The anti-pipeline group, Fossil Free Rhode Island has created a petition campaign directed at the Rhode Island Department of Health with the intention of blocking Spectra Energy's pipeline expansion and compressor station build-out. They urge the Department to use their mandate to protect public health. This expansion is part of the AIM Project, a proposed major expansion of the fracked natural gas infrastructure. Not only is this project part of a national energy policy that is potentially ruinous for life on Earth, but also it poses an imminent threat to the safety and health of the people of Rhode Island and of Burrillville in particular.

- Pennsylvania Governor Tom Wolf plans to sign an executive order ending a short-lived effort by his predecessor to expand the extraction of natural gas from rock buried deep below Pennsylvania’s state parks and forests, his office said Wednesday. Following through on a campaign pledge, Wolf will sign the order restoring a moratorium on new drilling leases involving public lands on Thursday at Benjamin Rush State Park in northeast Philadelphia.

- Three powerful accidents in recent years highlight weaknesses in the oversight of how natural gas providers maintain the largest pipelines in their networks, accident investigators said Tuesday as they issued more than two dozen safety recommendations. A major effort a decade ago by the federal government to check a rise in violent pipeline failures in “high-consequence” areas where people are more likely to be hurt or buildings destroyed has resulted in a slight leveling off of such
incidents, but no decline, the National Transportation Safety Board said.

- Community and environmental groups filed suit over the expansion of a crude oil operation in Kern County that could lead to a 1,000 percent increase in the amount of crude imported by rail into California each year. The newly opened Bakersfield Crude Terminal in Taft, Calif., has the capacity to receive two 100-car unit trains a day of volatile crude oil from the Bakken shale formation as well as heavier, highly toxic tar sands.

- Hundreds of indigenous Indians from the Peruvian Amazon demanded compensation for land use at 14 oil wells, where their demonstrations caused production to be suspended. Argentine oil company Pluspetrol said Wednesday. Some 300 to 400 indigenous people have been gathering at the oil wells near Peru's border with Ecuador since Tuesday. Pluspetrol said the demonstration had resulted in the suspension of production, and had also blocked transportation on a stretch of the Tigre River. The Indians, who blocked water access on the Tigre River, also retained eight company boats. Oil transport has proven difficult in the remote region, which can only be reached by plane or barges on the Amazonian rivers.

- The United Steelworkers union, which represents employees at more than 200 U.S. oil refineries, terminals, pipelines and chemical plants, began a strike at nine sites on Sunday, the biggest walkout called since 1980. The USW started the work stoppage after failing to reach agreement on a labor contract that expired Sunday, saying in a statement that it “had no choice.” The union rejected five contract offers made by Royal Dutch Shell Plc on behalf of oil companies including Exxon Mobil Corp. and Chevron Corp. since negotiations began on January 21. “The problem is that oil companies are too greedy to make a positive change in the workplace,” USW International Vice President Tom Conway said in the statement. “They continue to value production and profit over health and safety, workers and the community.”

- Algeria has been gripped by widespread protests against plans to frack the Sahara Desert.

- The 2015 Earth First! Winter Rendezvous event will be held February 20-23 in California, near the 101 freeway, in or near San Luis Obispo County. The specific location has not yet been announced.

- The Nuclear Regulatory Commission (NRC) has released the final two volumes of a five-volume safety report that concludes that Nevada’s Yucca Mountain meets all of its technical and safety requirements for the disposal of highly radioactive nuclear waste. “With reasonable assurance, subject to proposed conditions, DOE’s [Department of Energy] application meets the NRC’s regulatory requirements” for the disposal of “high-level nuclear waste,” the regulatory agency announced Thursday. However, “completion of the safety evaluation report does not represent an agency decision on whether to authorize construction,” the NRC noted, adding that DOE “has not met certain land and water rights requirements” and that other environmental and regulatory hurdles remain.

- The Huffington Post reports: Several unidentified flying objects have been spotted over nuclear power plants in France and Belgium over the last few months, and the story has been all over European news. Thus far, the media has reported that the UFOs are likely drones. However, currently, months after the sightings began, the French government still doesn't know who they belong to. Now a director of one of those nuclear power plants in France says whatever flew over his plant in October, 2014, was not a drone. It was a UFO. The media has reported that some authorities suspect the objects are drones flown by anti-nuclear activists to demonstrate that the plants are open to terrorist attacks via drones. However, authorities have not been able to track them. The largest anti-nuclear organizations have also denied any involvement.

- The House passed legislation to expedite the federal approval process for liquefied natural gas (LNG) exports. It was approved 277-133, with 41 Democrats voting in favor of the measure sponsored by Rep. Bill Johnson (R-Ohio). The Energy Department must determine whether each export application is within the country’s national
interest, thanks to a decades-old law written when gas was scarce. The United States is currently the top gas producer in the world. Under the bill, the Energy Department would have 30 days to review an application, starting from when the Federal Energy Regulatory Commission completes its environmental review for a project.

- Princeton University researchers have uncovered a previously unknown, and possibly substantial, source of the greenhouse gas methane to the Earth's atmosphere, writes John Sullivan in News at Princeton. "After testing a sample of abandoned oil and natural gas wells in northwestern Pennsylvania, the researchers found that many of the old wells leaked substantial quantities of methane. Because there are so many abandoned wells nationwide (a recent study from Stanford University concluded there were roughly 3 million abandoned wells in the United States) the researchers believe the overall contribution of leaking wells could be significant.

- The Scottish government has announced a block on planned fracking operations, pending further inquiries. Ministers will carry out new work on the environmental and health implications of the controversial gas drilling technique. Full control over fracking is due to be devolved to Scotland after May's general election. In the meantime, consent for unconventional oil and gas developments will be refused on planning grounds.

- In the coming months, Oklahoma's Supreme Court will decide whether two oil companies should be held financially responsible for injuries suffered by a woman during a 2011 earthquake thought to have been caused by drilling activity. If the woman's lawsuit is successful, it could set a legal precedent for future earthquake claims against oil and gas companies in Oklahoma.

---

**Agribusiness**

- Five environmental, animal welfare and community organizations filed suit in federal district court in Washington, DC, to force EPA to set air pollution standards for large livestock farms. The lawsuit asks the court to order EPA to act on a 2009 petition by the groups asking for the standards. "This failure to act is particularly egregious given the extreme risk to human health and welfare and the environment caused by aerial pollutants originating from CAFOs (confined animal feeding operations)," say the groups, the Humane Society of the United States, Association of Irritated Residents, Environmental Integrity Project, Friends of the Earth and the Sierra Club.

- Ukraine reached an agreement with exporters that would limit shipments of wheat used in flour out of the country in an effort to preserve food supplies.

- Falling grain prices continue to hurt John Deere. The Moline, Ill.-based Deere and Co. said Friday that it would lay off 910 workers in Iowa and Illinois, in yet another reduction in its American workforce. The newest layoffs will affect Deere facilities in Waterloo, Iowa; the Des Moines Works in Ankeny, Iowa, and the Harvester Works in East Moline, Ill. It represents the third round of layoffs at Deere, which cut more than 1,100 positions in the Midwest last summer as the farm economy slowed.

- Dairy wholesale prices in the UK have dropped again, undermined by a combination of bumper milk supplies and the strengthening pound against the euro.

- In South Korea reports have surfaced about the discovery of GM plant varieties found growing in 18 regions around the country. South Korea is becoming the world's second largest importer of GMO crops but has a ban on the cultivation of GMO's. The National Institute of Ecology (NIE) will be monitoring for GMO's around the country this year in order to stem the growing tide of unwanted GMO's growing in the country.

- Wilmar International Ltd. announced that it is making its palm oil supply chain transparent via a public web portal. The portal lists all palm oil suppliers from Indonesia and Malaysia.
In Minnesota, the bill SB 335 was introduced by Senators John Marty and Foung Hawj requiring the labeling of GMO's. According to the post the bill will be heard first in the Commerce Committee.

Sustainable Pulse reports that independent testing conducted on Kellogg’s Froot Loops has found “high levels of insecticide-producing genetically engineered corn” as well as the presence of glyphosate. Measurements of glyphosate reached levels of 0.12 mg/kg. This report comes as part of the organization GMO Free USA's Operation: Label GMO's which funds the testing of many mainstream food products for the presence of GMO's and associated pesticides.

The Institute for Ecosoc Rights, based in Jakarta, Indonesia released a report which has gained traction among environmental activist groups on social media. The report finds that spreading commercial palm oil “poses significant threats to livelihoods and the environment in rural provinces” where it is cultivated.

Monsanto Co. has long been a lightning rod for debate, but at its annual shareholder meeting Friday, the biotech-seed company was tagged with blame or credit for an even larger number of issues than usual. The sometimes emotional, nearly two-hour meeting sounded at times like a daytime talk show, minus thrown chairs and shouting. Critics charged Monsanto with responsibility for spikes in diabetes and autism, among other human and environmental problems. Springing to Monsanto’s defense were farmers, its own employees, and a nun who praised its efforts to reduce water use.

Insurance/Healthcare

- Federal regulators have unveiled a draft roadmap for achieving nationwide secure health data exchange built on interoperable electronic health records systems within the next three years.

- HealthcareInfoSecurity announced its third annual list of Top 10 Influencers to recognize leaders who are playing a significant role in shaping the way healthcare organizations approach information security and privacy.

- After heavy criticism from privacy watchdogs, the Department of Health and Human Services has made a number of fixes to the HealthCare.gov website for Obamacare to scale back the release of consumer data to third-party commercial sites.

- As the number of health data breaches continues to climb, the Department of Health and Human Services is taking steps to make the process of using online tools to report breaches more efficient, hoping that will help ease the launching of investigations.

Financial

**Financial Services**

**Activism**

- A two-day protest against income inequality and “outlandish” executive compensation will occur in Ridgewood, NJ on February 3. Participants will organize on the Ridgewood Avenue side of Van Neste Square (Memorial Park).

- A protest against a leading U.S. bank’s corruption and political influence occurred January 27 in San Francisco, CA. Participants brought a large mock check representing the millions the bank allegedly spent to “buy” the legislature during the 2014 election cycle, and demanded a meeting with the bank’s executives to return the money.
A housing activist group issued a call to action against banks to occur on Valentine's Day, February 14. Event details are yet to be disclosed.

An Atlanta, GA-based housing activist group is planning an anti-foreclosure demonstration in Lawrenceville, GA on February 3 in support of a homeowner facing eviction in Duluth.

Activists on January 31 held a demonstration at London City Hall to demand better homes for London residents.

A housing activist group is planning a demonstration outside City Hall in London, UK on February 23. Activists oppose the vote on a housing budget that the group believes will lead to high rents and the selloff of public land.

Numerous activist groups will conduct a series of protest actions from February 28 through March 3 against a lobbying group that advocates pro-Israel policies when Israeli Prime Minister Netanyahu visits Washington, DC to address them.

International activist groups will protest the U.S. and E.U. trade negotiators meeting in Brussels, Belgium on February 4. Protesters will demand European institutions stop the Transatlantic Trade and Investment Partnership (TTIP). The protest will occur at the Schuman roundabout at 10:30am local time and include a giant inflatable Trojan horse to symbolize "the dangers hiding inside TTIP."

A petition was launched to call on several major institutions, including financial firms, to pay the "heirs of African slaves reparations" for their involvement in the African slave trade.

An "activist marching band" delivered a petition with more than 100,000 signatures to the headquarters of a leading U.S. bank in New York City on January 28. The activists called on the bank and other financial institutions to remove terms in their contracts that deny customers their right to a day in court.

A Global Divestment Day campaign will occur February 13 -14 in cities across the globe as protesters will demand the fossil fuel industry stop funding fossil fuel expansion.

Information Security Risk

The Internal Revenue Service warned taxpayers to beware of a surge in fake emails or websites looking to steal personal information. The agency said these phishing schemes continue to be on their annual IRS list of “Dirty Dozen” tax scams for the 2015 filing season, and they won’t send customers an email about a bill or refund without advance notice.

Researchers said attackers are changing their tactics and moving towards sending users malicious links instead of malicious attachments. These malicious emails are also linked to the Cutwail botnet (Trojan.Pandex) and contain malicious URLs that lead to Downloader.Upatre, which in turn leads to the financial Trojan Infostealer.Dyranges (Dyre) being downloaded to the computer. However in some cases, users are instead of being sent to a site serving malware sent to a phishing page. Ultimately, however, the attackers’ goal is to steal information from victims’ computers as Infostealer. Dyranges is known to steal financial information and the phishing sites used in the attack campaign are masquerading as login pages for financial institutions.

An Indiana-based resort company announced on January 27 that malware infected its payment card system, and any guest who used their credit and debit cards at any venue at the resort between April 23, 2014, and January 21, 2015 may have had their personal information compromised.

An Indian bank launched a new payments service which enables customers to conduct 24/7 instant funds transfers by selecting recipients from their Twitter friends list.

Identity thieves are buying credit card numbers online, then loading the numbers into
their mobile payment service launched last year by an American mobile handset giant, in essence making themselves a handy fake credit card, without going through the trouble of making fake, physical credit cards. Researchers claim that for some issuers, fraud levels are as high as 6% (meaning $6 of every $100 spent is fraudulent), and it’s considered “bad” even when compared to regular credit cards, whose fraud rate averages out at under 1%.

- New research on the impacts of DDoS attacks revealed that the cost to businesses to resolve such attacks can often reach $444,000 (£293,000). The research found that, depending on the size of the company involved, DDoS attacks can cost businesses an average of $52,000 to $444,000.

- Researchers claim that an enhanced version of the infamous ZeuS Trojan, Trojan-Banker.Win32.Chthonic, or Chthonic for short, has hit over 150 different banks and 20 payment systems in 15 countries. The malware is targeting financial institutions in the UK, Spain, the US, Russia, Japan and Italy.

- Researchers found a malware toolkit that assumes control over a user's keyboard and mouse. Designed specifically for the banking sector, it conducts fraudulent payments without the user's knowledge. The malware, known as KL-Remote, is able to bypass such security measures as passwords. It tricks a number of detection tools, as they assume that the fraud is carried out from the hacker's device as opposed to the victim's. It is installed once the computer has been infected, and includes a number of pre-determined bank URLs. After the user has clicked one of the URLs, the toolkit notifies the hacker, who is then able to begin a phishing process. The user sees a pop-up message that looks exactly like the bank's login design and retrieves the user's details.

- Researchers discovered a new variant of the Zeus online banking malware that is targeting Canada's largest banks. This attack continues a growing trend in banking malware that goes beyond simply targeting the victim's login credentials (i.e. their username and password) and injects pages to steal a wealth of personal information including answers to security questions, debit and credit card numbers, social security number, driver's license numbers and more. This variant, like most banking Trojans, is not detected by anti-virus products. It also bypasses SSL browser security. Since the malware is installed on the endpoint device it can inject fake webpages into the browser without breaking the SSL connection to the bank's server and generating a security alert. Predictive execution technology that monitors activity on the endpoint device is the only way to detect and block these attacks, and protect personal information from getting into the hands of criminals.

**Legal, Litigation, Regulatory Risk**

- A Dutch judge ruled that an accused Russian “sophisticated hacker” can be extradited to the United States. The suspect, along with four other accomplices, four Russians and a Ukrainian, are accused of stealing credit and debit card numbers and other personal information from well-known U.S. companies and selling them online. Just three of the corporate victims have reported combined losses in excess of $300 million. The online theft case is reported to be one of the largest US corporate hacks of more than 160 million credit card details.

- A federal judge on January 28, 2014 said that U.S. investors may pursue a nationwide antitrust lawsuit accusing 12 major banks of rigging prices in the $5.3 trillion-a-day foreign exchange market. Six of the defendant banks have accepted more than $4.3 billion of civil fines from U.S. and European regulators, nine have banned traders from multibank chat rooms, and all 12 have overseen the suspension or departure of more than 30 employees linked to currency operations.

- U.S. securities regulators are considering charges against a leading U.S. bank, alleging it violated federal bribery laws by giving internships to relatives of foreign officials to win business managing investments for their country.

- An article reported that the Chinese government adopted new regulations requiring
companies that sell computer equipment to Chinese banks to turn over secret source code, submit to invasive audits and build so-called back doors into hardware and software. The new rules are the first in a series of policies expected to be unveiled in the coming months to strengthen cybersecurity in critical Chinese industries.

- The financial institutions in Canada that helped one of the leading commercial forest plantation operators in China raise funds have agreed to pay investors $32.5 million, in what may be the country's largest securities class action settlement to date reached with investment bank underwriters. The agreement, filed in court in Toronto on January 26th, is related to a lawsuit by investors who lost money when the Chinese forestry company collapsed amid allegations of fraud. The case alleged that directors, officers, auditors and underwriters at the timber company misled investors with its accounting. The allegations have not been proven in court and the agreement does not include any admission of wrongdoing. "The dealers make no admissions of liability and deny any liability in respect of the claims," the settlement agreement read.

- The Securities and Exchange Commission charged two employees of a leading U.S. bank of insider trading after they mined customer transaction data to successfully predict stock performance.

**Operational Risk**

- A U.S. ratings agency downgraded Russia to junk status for the first time in a decade due to collapsing oil prices, the tumbling value of the Ruble, and sanctions imposed because of its intervention in Ukraine. The agency said the downgrade was caused by the country's reduced flexibility to cut interest rates and a weakening of the financial system. Rival agencies have not pushed Russia's rating into junk territory although there are expectations that they will echo the decision.

- An article reported that one of the two GSEs for housing has announced the second sale of “deeply delinquent” mortgage loans worth approximately $410 million. According to the article, the conservator for the GSE is requiring reducing the number of delinquent loans and illiquid assets from its investment portfolio.

- In an effort to shift financial responsibility for a data breach at a community bank in Colorado, its insurer filed suit against the bank's web designer, claiming its negligence and "substandard" maintenance of a website set the stage for a breach. The insurance company asked in a claim that the website design studio pay $155,000 after it failed to put basic anti-malware on the bank's server, install critical software patches or maintain adequate encryption, among other deficits that it said led to hackers being able to breach the bank's server and gain access to the site.

- Two former foreign exchange traders from leading UK and German banks were charged in Singapore for allegedly cheating their employers by making false trades. The two men, in unrelated cases, bought and sold about $1.1 billion in U.S. dollars in November 2009 using the banks’ accounts to get preferential rates for themselves, according to documents filed Thursday, January 29th, with a Singapore state court. They allegedly made wrongful gains of about S$370,000 ($274,000).

**Global Intelligence**

**Brazil**

- Brazilian unemployment averaged 4.8% in 2014, down from 5.4% in 2013, and the lowest rate since the current methodology was adopted in 2002, the Brazilian Census Bureau (IBGE) said Thursday. December monthly unemployment was 4.3%, down from 4.8% in November. But economists warned that the figure does not necessarily presage an economic recovery in 2015, nor does it mean workers will earn more in real terms. Much of the decline in unemployment in 2014 was due to young Brazilians leaving the workforce and older workers taking early retirement. The total number of
registered workers in 2014 averaged 23.1 million, the same as 2013. Brazil's economy slowed to near zero growth last year on problems including persistent inflation, stagnant growth in wages and high interest rates.

- Petrobras started the week surprising and disappointing investors by declaring that they didn’t include any of the lost tens of billions in corruption in the calculations of their quarterly statement. U.S. stock and bond holders then filed suit in the U.S. against the company for securities fraud for failing to meet the required international accounting standards. The week ended with the Brazilian federal prosecutor issuing a warrant for the re-arrest of the Petrobras ex-Director of Services and the announcement that the dividend likely would not be paid pending a final decision in April.

- According to a recently published study, of the 90% taking selfies 12% take them daily, 58% once a week, and 29% less frequently. A majority, 72% like to take group “wefies” with friends and family in the photos. A majority of 68% posted them to social networks.

- Over ten different activist groups are uniting their efforts to have a large protest against political corruption at the congressional building in Brasilia. Lawmakers all return Sunday to be sworn in and elect their congressional leaders. Protesters plan to be there from 8 a.m. bussed in from five different states, with over 300 banners protesting corruption and calling for the impeachment of President Dilma.

- Protests organized by the Free Pass Movement (MPL) since price hikes on 5 January 2015 began peaceful but ended in violence. Military police moved to confront protesters with tear gas at the Faria Lima subway station in São Paulo during the January 27 protest against recent bus and subway fare increases. Military police estimated that 1,000 individuals participated in the protest while MPL estimated 10,000. Overall the protests were much smaller than the ones that swept the nation two years ago, the last time fare increases were attempted.

**Vietnam**

- Tuoi Tre News reported that a British newspaper ranked Ho Chi Miny City, Vietnam 48th on a list of cities considered safest in the world.

- Tuoi Tre News reported that Vietnam’s Ministry of Science and Technology has set aside more than 17 trillion VND ($792 million) for science and technology in 2015.

- Info.VN, a local VNeese media source, reported that Vietnamese security experts have confirmed that CTB-locker, a dangerous ransomware infection that decrypts files on computers and displays a so-called ransom warning, has turned up in Vietnam. According to renowned security expert in Vietnam, several agencies, including a large bank in Vietnam have been infected by the malware. After penetrating victims' computers, the malware will scan the computers' drives and encrypt files with public key cryptography. Most of the important files on the victims' computers with ".doc", ".pdf", ".xls", ".jpg" and ".zip" would not open.

- Info.VN, a local VNeese media source, reported that the Vietnamese government has warned that Vietnam’s energy future is at risk. A report by the Electricity of Vietnam (EVN) shows that while demand for energy to develop the economy remains high, the primary energy sources are diminishing in volume. Vietnam is seriously lacking power sources despite modest consumption compared with other countries.

### Legal and Regulations

- Verizon Wireless said it will allow customers to opt out of a supercookie tracking program used in its mobile phone browsers, Andrea Peterson reports for the Washington Post.
A committee established by Google is reviewing whether the decision by the European Court of Justice to enforce the “Right to Be Forgotten” on the internet be imposed beyond Europe’s shores? New York Times reports.


Pharmaceuticals

- Pfizer has reached an agreement in principle to pay $400 million to settle a class-action securities lawsuit that alleged the drug maker illegally marketed several medicines and, subsequently, caused investors to lose money, according to a filing with the U.S. Securities and Exchange Commission. The lawsuit alleged that, between January 2006 and January 2009, Pfizer marketed several drugs on an off-label basis.

- European regulators this week approved a complicated three-part transaction that would see Novartis and GlaxoSmithKline swapping parts of their companies and creating a consumer healthcare joint venture.

- As negotiators continue to shape the Trans-Pacific Partnership trade deal, the length of patent protection for biologics remains a sticking point with the U.S. continuing to push for 12 years of protection before a biologic drug can be copied.

Technology

- Automotive News reported that Toyota will change the way it pays factory workers, focusing on their performance rather than their seniority. According to the article, Toyota’s new policy was designed to attract young talent and will apply to about 40,000 employees, or about 60% of its workers aged between 18 and 65.

- Oregon Live reported that Intel announced its new program which allows for eight weeks of paid “bonding” time for all new parents, mothers and father alike. This is in addition to its new moms’ 13-week maternity leave.

- Facebook Inc. on Tuesday denied being the victim of a hacking attack and said its site and photo-sharing app Instagram had suffered an outage after it introduced a configuration change. The disruption “was not the result of a third party attack but instead occurred after we introduced a change that affected our configuration systems,” a Facebook spokeswoman told The Wall Street Journal. “We moved quickly to fix the problem, and both services are back to 100% for everyone.”

- US business groups are seeking “urgent discussions” over new Chinese rules requiring foreign firms to hand over source code and other measures. The groups wrote to senior government officials after the introduction of the cybersecurity regulations at the end of last year. The US Chamber of Commerce and other groups called the rules “intrusive”. The regulations initially apply to firms selling products to Chinese banks but are part of a wider review. “An overly broad, opaque, discriminatory approach to cybersecurity policy that restricts global internet and ICT products and services would ultimately isolate Chinese ICT firms from the global marketplace and weaken cybersecurity, thereby harming China’s economic growth and development and restricting customer choice,” the letter read.

- SailPoint uncovered a widespread level of employee indifference towards protecting sensitive corporate data, including personal information of customers. A survey confirmed that employees are lax about password management in general.
Dell SecureWorks Counter Threat Unit team observed the ZeroAccess botnet resumed with click-fraud activity.

Research team Qualys discovered a critical vulnerability in the Linux GNU C Library (glibc) that it would allow attackers to remotely take control of an entire system without having any prior knowledge of system credentials.

Researchers at Georgia Institute of Tech have developed a methodology which uses electromagnetic side-channel signals to attack a computer. The researcher explains that the EM signals can be used to compromised air-gapped computers. An example was the “AirHopper” method which captures EM radiation using mobile phone and sends the data to a remote server where it can be analyzed.

US Finance Post reported that AOL has announced that it will lay off around 150 people. The company is cutting back to help increase profit margins. An unnamed source has stated that the cuts will go far deeper than initial estimates with true figures above 200. Sales teams are the target of the layoff starting with the company’s leadership team on the west coast.

Fierce Telecom reported that Google Fiber confirmed that it would bring its 1 Gbps fiber-to-the-premises (FTTP) services to four new metro areas in the Southeast —Atlanta, Mashville, Charlotte and Raleigh-Durham, N.C. Google also confirmed that it is still considering bringing the FTTP service to four other cities, including Salt Lake City, San Antonio, Phoenix, and San Jose. Ultimately, the movement into those markets depends on its ability to get access to each city’s rights-of-way and a favorable permitting process to lay its fiber facilities.

Verizon agreed to a $5 million settlement after admitting that it failed to investigate whether its rural customers were able to receive long distance and wireless phone calls. The settlement is part of the Federal Communications Commission’s attempt to fix the rural call completion problem, which extends beyond just Verizon's network.

Germany’s leading telecommunications group said this week it keeps domestic Internet traffic within the country and sources key equipment from at least two suppliers. The steps are part of a series of privacy-protection measures Deutsche Telekom has introduced since large-scale wiretapping by intelligence agencies became public.

Prior to the New England Patriots facing the Seattle Seahawks in Super Bowl XLIX, researchers warned that at least one of the official National Football League (NFL) mobile applications is plagued by serious vulnerabilities that expose users’ personal information. According to Wandera, a company that provides mobile data gateway solutions for enterprises, the official NFL Mobile apps for iOS and Android are vulnerable to man-in-the-middle (MitM) attacks.

Federal agencies seized more than $19.5 million in fake NFL merchandise during ‘Operation Team Player’. 
A former CIA officer was convicted Monday of leaking details of a covert mission to derail Iran’s nuclear program in a case that, until the eve of the trial, was as much about the journalist who published the leaks as it was the accused leaker. The government gave up on its effort to force New York Times reporter James Risen to reveal his sources — and ultimately didn’t need him to win a conviction. Jurors convicted Jeffrey Sterling, 47, of O’Fallon, Missouri, of all nine counts he faced in federal court.

A keylogging module that works with WARRIORPRIDE, a malware platform known to be used by the US National Security Agency (NSA), has been found to share a large chunk of source code with a component present in Regin malicious toolkit. WARRIORPRIDE is not used by the NSA exclusively, as it appears to be shared by the intelligence agencies of the nations part of Five Eyes (the US, UK, Canada, Australia and New Zealand).

The Defense Department is accelerating toward wide-scale cloud computing adoption, buoyed by the promises of cost savings and untold increases in mission capabilities.

An annual report released by the Pentagon’s chief weapons tester indicates that a majority of the government’s weapons programs contain “significant vulnerabilities.”

Amid reports of Australia deploying cyber weapons in the Middle East in a counter-terrorism operation, a cyber-espionage program was discovered being used by several countries in sophisticated hacking operations. Security experts revealed the existence of the spying software after former NSA contractor Edward Snowden allegedly leaked the source code.

**Law Enforcement**

- New York Police Department Commissioner William J. Bratton announced Thursday a new unit specifically created to respond to protests and terrorist attacks. According to the New York Times, the Strategic Response Group, comprised of around 350 officers, will be equipped with machine guns and heavy armor and will receive training in advanced counterterrorism tactics and “disorder control.” Bratton cited the recent terror attacks in Paris as one example of the type of large-scale incidents the new unit will be trained to respond to.

- Sheriffs said Wednesday that Google’s popular Waze traffic app is making it harder to nab speeders, adding to earlier police complaints that a feature in the software that lets drivers warn others about nearby police activity is putting officers’ lives at risk. The National Sheriffs’ Association had previously focused its campaign against Waze on police safety after the fatal shootings of two New York police officers in December. It broadened its campaign with a new statement criticizing Google’s software as hampering the use of speed traps. The trade association said radar guns and other speed enforcement techniques have reduced highways deaths.

- The FBI says it is trying to determine who made online threats involving three commercial airline flights, causing the evacuation of two and the diversion of another. FBI spokeswoman Laura Eimiller said Monday that agents were investigating whether the threats came from the same person or from copycats. Law enforcement determined the public was not at risk. Passengers were taken from two planes that landed at Seattle-Tacoma International Airport. In addition, a Delta Air Lines flight was diverted to Dallas from its Los Angeles-Orlando, Florida, route.

- Pedro Leonardo Mascheroni, a former scientist at the Los Alamos National Laboratory (LANL) in New Mexico, was sentenced Wednesday to five years in prison for leaking classified nuclear weapons data to a person he believed to be a Venezuelan government official.
A license plate tracking program established to seize cars and money to combat drug trafficking has gone far beyond its original scope and has led to the collection and storage of millions of records about motorists, Reuters reports. Not only is the database being used to track drug dealers, but state and locals authorities are using it to search for cars tied to other serious crimes, raising questions among privacy advocates.