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

Join Cyveillance and Centripetal Networks as we explore the challenges in closing the breach detection gap, managing large dynamic sets of threat intelligence, and how to operationalize threat intelligence in a perimeter defense strategy.

Date: April 9, 2015
Time: 1:00 PM ET

Top Incidents

**Energy**

- The anti-fracking Energy Justice Shale Convergence is scheduled for March 13-16 in PA. Organizers of this event and the Shalefield Justice Spring Break event taking place on March 6-13 are cross-promoting and encouraging activists to attend both.

**Agribusiness**

- In early 2015, many US state legislation’s have quickly proposed anti-GMO or GMO-labeling bills for consideration. While there are still ongoing efforts on the national level, much activity surrounding GMO’s have becoming noticeably focused on state-level legislation.
• The potential legal liabilities from the unprecedented breach of some 80 million individuals’ records at Indianapolis-based insurance giant Anthem could entangle nearly 60 health insurance plans from Hawaii to Puerto Rico, legal experts say. More than 50 class-action lawsuits related to the breach already have been filed in less than a month.

**Financial Services**

• The FBI and the State Department announced a record $3 million reward Tuesday, February 24, for information leading to the arrest of a Russian accused of executing a sophisticated computer heist that siphoned more than $100 million from American bank accounts. The accused, Evgeniy Bogachev, who is believed to be in Russia, was charged last year and in 2012 with computer crimes. He was already on the FBI’s “Cyber’s Most Wanted” list. The $3 million bounty is the highest ever for an alleged cybercriminal. The 31-year-old fugitive, who authorities say used the online monikers “lucky 12345” and “slavik,” is accused of deploying malicious software known as GameOver Zeus, which is designed to steal bank account numbers and passwords.

**Global Intelligence**

• What began with a tiny artificial island built by China to stake a concrete claim in the South China Sea is fast on its way to becoming 600 acres of at least seven islands spread across the South China Sea. One of the most impressive is so-called Fiery Cross Island, the permanent structure above complete with an air strip and, perhaps, the ability to permanently station advanced weapon systems there to patrol the skies and seas.

**Legal and Regulations**

• The U.S. Securities and Exchange Commission is debating whether to impose lifetime bans on executives who violate securities rules.

**Pharmaceuticals**

• A study by a Timothy Libert, a doctoral student at the University of Pennsylvania, has found that nine out of ten visits to health-related web pages result in data being leaked to third parties like Google, Facebook and Experian.

**Retail**

• When it comes to data breaches, retailers are one of the biggest targets these days, and now we have some detail on the costs around one of the more high-profile attacks. Target Thursday said that it has booked $162 million in expenses across 2013 and 2014 related to its data breach, in which hackers broke into the company’s network to access credit card information and other customer data, affecting some 70 million customers.

**Technology**

• A new targeted phishing campaign has been observed by security researchers to focus on high level security professionals in technical companies, such as CTOs. Researchers at Talos, Cisco’s security intelligence and research group, observed on Tuesday the deployment of the malicious campaign, which delivered emails with subjects related to different payment details and federal taxes.

**Telecommunications**

• FairPoint Communications has made yet another step forward with its labor unions, announcing that after three days of voting, the International Brotherhood of Electrical Workers (IBEW) and the Communications Workers of America (CWA) have ratified tentative agreements with the telco.

**Defense**
President Obama Wednesday directed the Director of National Intelligence (DNI) to establish the Cyber Threat Intelligence Integration Center (CTIIC). The CTIIC will be a national intelligence center focused on "connecting the dots" regarding foreign cyber threats to the nation and cyber incidents affecting U.S. national interests, and on providing all-source analysis of threats to U.S. policymakers. The CTIIC will also assist relevant departments and agencies in their efforts to identify, investigate, and mitigate those threats.

**Law Enforcement**

Servando "La Tuta" Gomez, a former school teacher who became one of Mexico's most-wanted drug lords as head of the Knights Templar cartel, was captured early Friday by federal police as he tried to sneak out of a house in Morelia, the capital of the western state of Michoacan. He was arrested along with eight bodyguards and associates toting a grenade launcher, three grenades, a machine pistol and assault rifles.

**Energy**

- Anti-fracking activists crashed a Colorado oil and gas task force meeting this past Tuesday to launch a campaign for a statewide fracking ban. Organizers are hoping for an eventual ballot measure.

- Organizers for the anti-fracking Shalefield Justice Spring Break event (March 6-13 in PA) have released a detailed agenda. The agenda includes workshop names.

- The anti-fracking Energy Justice Shale Convergence is scheduled for March 13-16 in PA. Organizers of this event and the Shalefield Justice Spring Break event (March 6-13) are cross-promoting and encouraging activists to attend both.

- Greenpeace New Zealand is promoting a March to Stop Deep Sea Oil on March 19.

- Deep in the Algerian Sahara, daily protests against a pilot hydraulic fracturing project are now well into their second month. The demonstrations have spread to several towns and have provided opposition parties with a new platform at an especially precarious moment for the government, as oil prices have slumped and the declining health of President Abdelaziz Bouteflika has removed him almost completely from public view.

- Google is once again boosting its investment in SolarCity's residential solar power model by $300 million, both companies announced Thursday. Combined with a new financing structure from SolarCity, the companies say this will result in a new fund worth $750 million to help install distributed rooftop solar on homes across the country.

- The 28 member states of the European Union are to integrate their markets and increase security of supply under a policy set known as the Energy Union. Investments of €200 billion ($227 billion) per year are expected over the next decade. The Energy Union is a flagship project of the new president of the European Commission Jean-Claude Juncker, whose vice president Maroš Šefčovič is in charge of achieving the Energy Union goals. Documents announcing the strategic framework for the project said: "Today the European Union has energy rules set at the European level, but in practice it was 28 national regulatory frameworks. This cannot continue."

- World Nuclear News reports that legislation to cut carbon emissions currently before the Illinois general assembly would ensure the continued operation of the state's nuclear power plants, according to Exelon. Bills introduced in both the state Senate and House over the past week would enact the Illinois Low Carbon Portfolio Standard, helping to reduce carbon emissions, increase renewable energy and maintain a stable and secure electricity supply in the state. Under the proposed legislation, utilities will be required to purchase low-carbon energy credits equivalent to 70% of the utility's annual retail sales to customers within the state. Qualified sources include energy from
solar, wind, hydro, nuclear, tidal, wave and clean coal. Although the legislation would allow utilities to recover the costs associated with the purchase of low-carbon credits through charges, it would also put in place safeguards such as a consumer price cap to protect customers. It will also pave the way for future steps the state may need to take to meet the requirements of proposals by the US Environmental Protection Agency (EPA) to cut power plant carbon emissions by 30% by 2030.

- The Vancouver observer has posted (2/23/215) this article discussing the result of a Freedom of Information (FOI) request by ICBC CEO Robyn Allan on senior-level meetings between the federal government and Kinder Morgan. Three of the meetings involved then-Natural Resources Minister Joe Oliver. Allan filed FOI requests on records relating to 20 meetings between Kinder Morgan and the federal government in 2013 and 2014 in May, and received her first response in October. The request turned up no records, agenda, minutes, or briefing notes. The document obtained by Allan had communications for five junior-level meetings, which contained the information Allan expected to find. However, the majority of the meetings had no records. "What shocks me is that no records that exist. We're not even talking about withholding information. They said: 'we have no paper documentation at all.' There's no trail, no way to hold anyone to the truth." And that's dangerous, Allan said. "It's a betrayal of public trust."

- Aboriginal Peoples Television Network (APTN) has posted this article discussing the proposed anti-terrorism bill (C-51) and the reaction to it by Indigenous grassroots leaders. Indigenous leaders are concerned with wording in the bill that equates "interference with critical infrastructure" to terrorism. NDP leader Tom Mulcair has also raised concern with the bill's vague language, particularly in definition of 'terrorism'. Those indigenous leaders quoted in this article are not deterred by C-51. In fact, Clayton Thomas-Muller, Co-Director of the Indigenous Tar Sands Campaign, suggested that the bill is a response to the success of the Indigenous movement.

- Yahoo News reports one of three Al-Jazeera journalists arrested for flying a drone in Paris will appear in court next week after pleading guilty, a judicial source said on Thursday. The other two television journalists have been freed. All three were arrested on Wednesday for flying a drone in the Bois de Boulogne park on the western edge of the French capital, for the purposes of a television report. Those unexplained sightings were made near the US embassy, not far from the Invalides military museum, the Eiffel Tower and several major thoroughfares leading in and out of the French capital, police said. The journalist facing court is a 34-year-old British citizen working for Al-Jazeera's international service, who received the drone from the station's London bureau in November. The unmanned aircraft has been confiscated by the authorities.

- The New York Times discusses Wei-Hock Soon, known as Willie, a scientist at the Harvard-Smithsonian Center for Astrophysics who claims that variations in the sun's energy can largely explain recent global warming. The NYT reports that newly released documents show the extent to which Dr. Soon's work has been tied to funding he received from corporate interests. They explain that Mr. Soon has accepted more than $1.2 million in money from the fossil-fuel industry over the last decade while failing to disclose that conflict of interest in most of his scientific papers. At least 11 papers he has published since 2008 omitted such a disclosure, and in at least eight of those cases, he appears to have violated ethical guidelines of the journals that published his work. The article goes on in further detail to summarize Mr. Soon's ties to the fossil fuel industry.

---

**Agribusiness**
State investigators have concluded an investigation into a huge fire that killed more than 12,000 pigs and hogs at a southern Minnesota swine farm. The State Fire Marshal Division released its conclusion Tuesday that the blaze at Cougar Run near Truman in Martin County was accidental and caused by excessive heat from pressure washers.

Portions of the Renewable Fuels Standard that effectively mandate the use of corn-based ethanol would be repealed under a bill introduced by Sens. Dianne Feinstein of California, Pat Toomey of Pennsylvania and Jeff Flake of Arizona.

After months of negotiations and threats of an economically disastrous shutdown, the news of a “tentative agreement” in the West Coast port dispute came as a relief to many in the agriculture industry.

The European Commission has taken Italy to court for not collecting €1.34bn (£1bn) of fines for bursting through its milk quota.

On February 23, 2015, Friends of the Earth International released a report detailing efforts by NGO's, corporations, and the US government to promote GMO sales to countries in Africa. The report describes companies like Monsanto and the US government's efforts to promote GMO-friendly legislation in African nations. At this time, only South Africa, Egypt, Burkina Faso and Sudan allow GMO's to be sold commercially.

Friends of the Earth Europe reported that farmers in Uganda evicted by oil palm plantations presented a lawsuit against a joint venture co-owned by the oil palm giant Wilmar International. They are claiming restitution for their grabbed land and fair compensation for damages, three years after their land was taken for plantation development. Friends of the Earth International is backing the communities' land grab case, filed after three years of dialogue with the government and the company.

There has been continued activity on social media from activist groups opposing GM apples that were approved in the US in mid-February. Activists in Canada are calling for their markets to stay closed to the GM apples.

In early 2015, many US state legislations have quickly proposed anti-GMO or GMO-labeling bills for consideration. While there are still ongoing efforts on the national level, much activity surrounding GMO's have becoming noticeably focused on state-level legislation.

This is Africa reported that Africa's food imports are increasing and food self-sufficiency is declining. This should create substantial local and regional marketing opportunities for African farmers and this will include smallholders, but only if certain conditions are met.

In Massachusetts, 154 out of 200 legislators have signed on to sponsor the Genetic Engineering Transparency Food & Seed Labeling Act - temporary Docket #HD369.

Illinois Sen. Dave Koehler has introduced SB 0734, a bill to label GMOs in Illinois. Nine Senators - John Mulroe, Jacqueline Collins, Terry Link, Emil Jones III, Julie Morrison, Dan Kotowski, Patricia Van Pelt, Heather Steans and Michael Noland have signed on as co-sponsors.

Sustainable Pulse reported that the USDA and Canada’s CFIA are currently reviewing GMO Arctic Golden and Arctic Granny apples, with both expected to be approved for cultivation in 2014. However, a source revealed that an EU Directive regarding the antibiotic marker gene Kanamycin, found in the GMO Arctic Apples, could threaten not just North American future GMO Arctic Apple exports but the whole of the North American apple export market to the EU. It could also threaten exports to China, Russia, Mexico and Costa Rica due to similar regulations.

In the continued campaign against PepsiCo, Quaker Oats Chewy Bar product is the Rainforest Action Network's latest target for allegedly using conflict palm oil.
Hershey’s announced the company will be removing artificial flavors (vanillin) and the emulsifiers PGPR and moving to non-genetically modified sugar and milk from cows that have not been treated with rBST in Hershey Chocolate Bars and Kisses by the end of 2015.

Insurance/Healthcare

- A class action lawsuit has been filed against Hospital Corporation of America - which owns the Aventura (Fla.) Hospital and Medical Center, where the breach occurred, and Envision Healthcare - in a case involving an insider breach that affected more than 82,000 individuals and allegedly went on for about two years. The plaintiffs claim they did not receive the data privacy protections that they “paid for” and that was promised to them by the hospital involved.

- As the healthcare industry continues to digitize patient records, that data is a growing target for cybercriminals intent on committing medical identity theft and fraud.

- Health insurer Anthem Inc., which earlier this month reported that it was hit by a massive cyberbreach, said on Tuesday that 8.8 million to 18.8 million people who were not its customers could also be victims in the attack.

- Scottish ministers have been accused of introducing a central database by stealth after civil servants quietly published plans to expand an NHS register to cover all residents and share access with more than 100 public bodies, including HM Revenue and Customs (HMRC).

- The Senate passed a bill Tuesday that is designed to stop police from snooping without a warrant into a state database that records Utahans’ prescription medicines.

- The potential legal liabilities from the unprecedented breach of some 80 million individuals’ records at Indianapolis-based insurance giant Anthem could entangle nearly 60 health insurance plans from Hawaii to Puerto Rico, legal experts say. More than 50 class-action lawsuits related to the breach already have been filed in less than a month.

- Earlier this year, the California Department of Public Health (CDPH) announced it had issued monetary penalties against multiple hospitals after investigations into privacy breaches.

- A former Texas hospital worker has been sentenced to 18 months in federal prison for criminal HIPAA violations, one of the toughest penalties yet for that crime. And some legal experts predict more criminal prosecutions for HIPAA violations are likely.

Financial

Financial Services Activism

- Occupy Wall Street offshoots ‘OWS S17’ and ‘Occu-Evolve OWS’ hosted a planning assembly on February 27 in NYC to finalize actions planned for “important” events happening in the city, including a City-Wide and National Shutdown for Justice and Boycott, May Day. Two Big Marches in Staten Island to commemorate the 50th Anniversary of the Selma March, and a proposed City-Wide March on City Hall.

- Activists conducted a “Moral Monday” rally to raise the minimum wage in Atlanta, GA on February 23. Another minimum wage rally is scheduled to take place on April 15.

- Activists held an anti-austerity demonstration in Detroit, MI on February 23.
Activists in Seattle held a protest march to Burien City Hall Council Chambers on February 23 in Burien, WA against the city’s Ordinance 606 targeting homeless people.

Activists held a protest on Sunday, March 1, in front of Canada’s central bank in Calgary, Alberta, Canada against Canadian government for allowing international groups to print Canadian money and then charge an exorbitant amount of interest on it. Participants also called on the exposure of an anti-Terror Bill that will allegedly give Canadian spies police-like powers to disrupt terrorist operations and bring attention to the lawsuit that aims to restore the use of the Bank of Canada.

‘OWS S17 2015 and Occu-Evolve_OWS’ held a ‘#EndKettlingofDissent’ protest in New York, NY on February 28. Participants protested being restricted to a small area during a previous protest at the same location on January 2nd.

Occupy Fights Foreclosures (OFF) held a protest against the proposed merger of two financial institutions at the Federal Reserve Bank of Los Angeles building in California on February 26. The group called this a 'Too Big To Fail Bank Merger.'

A 'Court Support' rally organized by 'FloodWallStreet' for 11 of the #FloodWallstreet arrestees who have refused a plea deal and pled 'not guilty' to disobedience charges from the sit-in at Broadway and Wall St. occurred at the 100 Centre St courthouse in NYC on March 2nd.

**Information Security Risk**

Two former security employees at a company that makes a popular tax preparation software alleged that the company has made millions of dollars knowingly processing state and federal tax refunds filed by cybercriminals.

The world's largest provider of high-security mobile-phone and bank-card chips said U.S. and U.K. spies were probably behind the most sophisticated computer attacks on its networks in at least five years though they failed to steal a large amount of data. The company downplayed the significance of the hacking attempts, insisting that the attackers failed to get inside the network where cryptographic keys are stored that protect mobile communications. Many in the information security community, however, criticized the company for asserting this after such a short investigation, particularly since the U.S. spy agency has been known to deploy malware and techniques capable of completely erasing any signs of an intrusion after the fact to thwart forensic discovery of a breach.

A global credit card service provider is set to debut a new mobile payments service in Europe in April that will tokenize payment card data. The move is designed to enable consumers to use their smart phones and wearable devices to securely pay retailers. Tokenization refers to the practice of transmitting a unique, one-time token in place of card data whenever a transaction gets made. And unlike physical cards, the credit card service provider noted that the use of a particular token can be restricted to certain types of scenarios. For example, banks might prohibit a token created for contactless payments from being used for online purposes. Experts said that making tokenization mainstream, as well as implementing end-to-end encryption to secure data during transit, will be crucial for improving payment card security and combating fraud.

A study showed that today over 70% of the 25 most downloaded mobile apps identified as vulnerable to Man in the Middle attacks last year have still not been fixed, potentially affecting millions of users. The study said in 2014 over 20,000 Android apps failed to validate SSL certificates via HTTPS properly, exposing them to MITM attacks.

A new report revealed that less than a third (31%) of all organizations studied discovered an internal breach themselves last year, with 69% notified by a third party. Yet the median number of days hackers were present on the network before discovery dropped from 243 in 2012 to 229 in 2013, and went down again last year to 205 days. Interestingly, when it comes to the phishing attacks that so often start a major targeted incursion, the study found that the vast majority (78%) were IT or security related. The
messages were spoofed to appear as if they came from the victim company’s IT department or AV vendor. Unsurprisingly given the huge number of targeted attacks aimed especially at US retailers, this sector displayed a spike in data breach incidents last year.

- Cyber criminals are stealing secret algorithms and tactics used by hedge funds and high-frequency trading firms. Such algorithms are designed to take advantage of infinitesimal price discrepancies in the stock market that may only last for milliseconds. The algorithm information can be used for a few different nefarious purposes, including blackmailing a company into buying back its own data; or, selling it to other traders on the black market.

- Phishers are sending out links that, when clicked, quietly alter the settings on vulnerable routers to harvest online banking credentials and other sensitive data from victims. Researchers detected a four-week spam campaign sent to a small number of organizations and targeting primarily Brazilian Internet users. The emails were made to look like they were sent by Brazil’s largest Internet service provider, alerting recipients about an unpaid bill. In reality, the missives contained a link designed to hack that same ISP’s router equipment.

- Researchers have discovered a vulnerability that allows attackers to turn Joomla servers using the Google Maps plugin into a DDoS hacking tool. The technique known as Joomla Reflection DDoS is low cost and easy to run. During the fourth quarter of 2014, researchers observed 39 percent of all DDoS attack traffic used reflection techniques, which take advantage of an Internet protocol or application vulnerability that allows DDoS attackers to reflect malicious traffic off a third-party server or device.

- An American cosmetics company began notifying an undisclosed number of customers that unauthorized access was gained to its website server and malware designed to intercept customer data, including payment card information was installed from October 2014 to February this year. The incident affected customers who made purchases on the company website between October 4, 2014 and February 15. The company said for customers that used an online digital wallet service to make purchases, the company website usernames and passwords may have been obtained, but credit or debit card information was not captured by the malware.

- A UK broadband and phone company, which has over four million customers, said data including addresses, account information and phone numbers were leaked when a third party contractor - that had legitimate access to its system - was involved in a data breach during 2014. While no bank details have been leaked directly, customers have had money stolen from their accounts indirectly, after online criminals used the stolen data to contact customers and trick them into giving hackers access to their bank accounts.

Legal, Litigation, Regulatory Risk

- The largest U.S. bank said that it was questioned on Tuesday, February 24 by the U.S. Department of Justice over auto lending practices that possibly resulted in discrimination. The bank said in an annual filing with the U.S. Securities and Exchange Commission that the Justice Department is looking at whether auto loans made by car dealerships to borrowers of different races and ethnicities may have been marked up.

- A leading U.S. bank said that the U.S. Justice and Treasury departments are looking into possible money-laundering violations at the company. The bank said that the Justice Department is also reviewing its subprime auto finance business. The McLean, Va., company said that the federal authorities had asked for the information in “early 2015,” according to a regulatory filing.

- A leading U.S. investment firm agreed to pay $2.6 billion to settle claims linked to the housing bubble that triggered the 2008 financial crisis. The U.S. Department of Justice claimed the investment bank was packaging bad loans into mortgage-backed securities, misrepresenting their quality. In a regulatory filing, the firm said the settlement would cut its 2014 profit in half, slashing earnings from continuing operations by $1.35 per share. It had reported EPS of $2.75 in January.
A leading U.S. bank agreed to pay $7 billion to settle charges that it packaged bad mortgages during the run-up to the financial crisis. It includes $4 billion in penalties, $2.5 billion in mortgage modifications and other relief to homeowners, and $500 million going to five states and the Federal Deposit Insurance Corp.

The US Department of Justice said on Tuesday, February 24 that a senior vice president of a leading U.S. bank pleaded guilty to abuse of funds that resulted in a loss of millions of dollars. The former executive who was in charge of the bank’s Las Vegas operations pleaded guilty to misapplication of bank funds in a scheme that led to over $6.4 million in losses to the bank on two business-related loans.

The third-biggest U.S. bank said that an investigation into money-laundering controls at one of its subsidiary units has expanded, with additional U.S. and state authorities seeking information. The bank and the subsidiary received requests for information from the U.S. Treasury Department’s Financial Crimes Enforcement Network and California’s Department of Business Oversight in an annual regulatory filing. The bank said last year it got subpoenas related to compliance with the Bank Secrecy Act and federal anti-money-laundering requirements from the U.S. Attorney’s Office for the District of Massachusetts and the Federal Deposit Insurance Corp. The bank’s subsidiary unit is grappling with probes of its U.S. arm and alleged loan fraud in Mexico that prompted employee firings and cost the firm more than $400 million.

The FBI and the State Department announced a record $3 million reward Tuesday, February 24th, for information leading to the arrest of a Russian accused of executing a sophisticated computer heist that siphoned more than $100 million from American bank accounts. The accused, Evgeniy Bogachev, who is believed to be in Russia, was charged last year and in 2012 with computer crimes. He was already on the FBI’s “Cyber’s Most Wanted” list. The $3 million bounty is the highest ever for an alleged cybercriminal. The 31-year-old fugitive, who authorities say used the online monikers “lucky 12345” and “slavik,” is accused of deploying malicious software known as GameOver Zeus, which is designed to steal bank account numbers and passwords.

Operational Risk

This month, the World Bank Group announced the debarment of four companies involved in misconduct relating to projects in Bolivia, Bangladesh and Cambodia. The debarments were announced by the Sanctions Board following investigations by the World Bank’s Integrity Vice Presidency (INT).

The head of New York’s Department of Financial Services (DFS) said he is considering new rules to protect against "an Armageddon-type" cyber-attack that would devastate U.S. financial markets. The chief regulator said he wants to add cyber security to the grades DFS gives the banks and insurance companies it regulates. Financial firms "care deeply" about their grades because they can impact their ability to pay dividends or acquire other companies. DFS could also mandate multifactor authentication systems for employees of DFS-regulated financial firms. Single-step passwords "should have been dead and buried many years ago," the regulator said. DFS may also require banks and insurance companies licensed by the agency to get guarantees from third-party vendors that their security meets certain standards. Such vendors can often acts as a "backdoor entrance for hackers," he said.

Starting March 10, a leading UK bank will allow customers to make payments to each other and small businesses using only their Twitter handles.

Reputational Risk

An article claimed that the largest online retail mortgage lender headquartered in Detroit, Michigan contributed to the financial crisis long faced by its home city of Detroit. The article stated that over 70% of homes that had borrowed from the retailer as their original mortgage went into foreclosure within the first 24-36 months of being sold on the secondary housing market to either one of the two GSEs for housing.

A parody of the movie 'Hunger Game' produced by employees of a leading U.S. bank was leaked to the public by a financial news organization. The video provides behind-
the-scenes look at the country's largest wealth management firm. The 10-minute video reflects a cutthroat culture among wirehouse managers and a lack of congeniality between leaders in the field and executives in the home office. Some current and former executives of the firm said the fact that a video was even made that joked about people who were losing their jobs shows the detachment of executives from other employees.

- A former broker for a leading U.S. investment firm filed a suit accusing the company of firing him for being a whistleblower. He claims he was terminated for raising allegations of insider trading involving its Knoxville, Tenn., branch and for helping federal authorities uncover fraud at a truck-stop chain.

Global Intelligence

Brazil

- Brazil's government will start fining truckers as a strike now in its ninth day threatens Latin America's largest economy with food and fuel shortages.

- Brazilian unions have filed suit alleging that the largest operator of McDonald's restaurants in Latin America violates Brazil's labor laws, a case that could lead to fines of up to 30 percent of annual sales. The suit is backed by two of Brazil's largest labor federations, CUT and UTG, as well as the Washington, DC-based Service Employees International Union (SEIU). The issue is an outgrowth of the U.S. minimum wage initiatives of U.S. unions.

- Under Brazilian law, lawmakers and cabinet members can only be tried by the Supreme Court. Prosecutor Rodrigo Janot has said he plans to file cases with the court by the end of the month against politicians involved in the graft scheme at Petrobras. Who will be on Janot's list has become a nervous guessing game for Brazil's political class. The corruption scandal has already hit Brazil’s business class. The investigation has so far led to 39 indictments for racketeering, bribery and money laundering. Moody’s cut Petrobras’ credit rating to junk, level Ba2 and warned further reductions were possible. The new rating will bar by rules many institutions from holding the stock.

- Beginning Monday electricity consumers will begin to feel the effects of the government's new so called “realistic rates” in an extraordinary rate adjustment that will have an average effect of a 23.4 percent rise in electricity bills. The rise is primarily due to the 46 percent increase in the price of energy from the Itaipu hydroelectric dam due to the longest drought since 1930 affecting energy production across the country.

China

- What began with a tiny artificial island built by China to stake a concrete claim in the South China Sea is fast on its way to becoming 600 acres of at least seven islands spread across the South China Sea. One of the most impressive is so-called Fiery Cross Island, the permanent structure above complete with an air strip and, perhaps, the ability to permanently station advanced weapon systems there to patrol the skies and seas.

- An article on 163.com reports a malware targeting Android devices called PowerOffHijack is able to hijack the shutdown process of Android devices and make the devices appear to have been turned off but in fact it is still turned on to make unauthorized phone calls, takes pictures and send text messages.

- An article on ETtoday.net reports that the Chinese Communist Cyber Army frequently targets Taiwan's National Security Agency. Within a year, the Chinese Communist Cyber Army launched 7,226,657 attacks, including 238,764 malicious attacks against Taiwan's National Security Agency's official website.
A Chinese news outlet reported that Trend Micro identified a hacker group located in the Jilin, Yanbian region of China. The group exploited a malicious source code targeting Korean mobile phone users in order to steal personal information.

**Malaysia**

- An article on Free Malaysia Today reports several unions are expected to protest against the layoff of 6,000 Malaysian Airline workers.
- An article on Malaysian Insider reports the Good and Services Tax will be exempted from any high-rise residential units. The Good and Services Tax will take effect on April 1 of this year.

· Brazil’s government will start fining truckers as a strike now in its ninth day threatens Latin America’s largest economy with food and fuel shortages.

· Brazilian unions have filed suit alleging that the largest operator of McDonald's restaurants in Latin America violates Brazil’s labor laws, a case that could lead to fines of up to 30 percent of annual sales. The suit is backed by two of Brazil’s largest labor federations, CUT and UTG, as well as the Washington, DC-based Service Employees International Union (SEIU). The issue is an outgrowth of the U.S. minimum wage initiatives of U.S. unions.

· Under Brazilian law, lawmakers and cabinet members can only be tried by the Supreme Court. Prosecutor Rodrigo Janot has said he plans to file cases with the court by the end of the month against politicians involved in the graft scheme at Petrobras. Who will be on Janot’s list has become a nervous guessing game for Brazil’s political class. The corruption scandal has already hit Brazil’s business class. The investigation has so far led to 39 indictments for racketeering, bribery and money laundering. Moody’s cut Petrobras’ credit rating to junk, level Ba2 and warned further reductions were possible. The new rating will bar by rules many institutions from holding the stock.

· Beginning Monday electricity consumers will begin to feel the effects of the government’s new so-called “realistic rates” in a extraordinary rate adjustment that will have an average effect of a 23.4 percent rise in electricity bills. The rise is primarily due to the 46 percent increase in the price of energy from the Itaipu hydroelectric dam due to the longest drought since 1930 affecting energy production across the country.

**Legal and Regulations**

- The Federal Communications Commission voted along party lines to regulate the internet as a public utility, Rebecca R. Ruiz and Steve Lohr report for the *New York Times*. Internet service providers such as Comcast and Verizon are expected to challenge the FCC’s net neutrality rules in court, Siobhan Hughes reports for the *Wall Street Journal*.

- The U.S. Securities and Exchange Commission is debating whether to impose lifetime bans on executives who violate securities rules.

- The White House unveiled its long-awaited consumer data privacy bill, which drew immediate criticism from privacy advocacy groups who say the measure doesn't go far enough, Natasha Singer reports for the *New York Times*. Even the Federal Trade Commission raised concerns, the *Washington Post*’s Andrea Peterson reports.

- ICANN new gTLD auction resulted in the largest amount ever paid for a TLD when Google purchased .app for a record-breaking $25 million. According to a *DomainNameWire.com report*, twelve companies were bidding for the domain name during ICANN’s auction on Wednesday, with Google eventually out-bidding other applicants, including Amazon.com, Minds + Machines and Radix. The .app domain name is a natural fit with the Google Play Store now that Google is an official domain registrar. The company opened its domain services to all users last month, after
launching its invite-only domain service in June of last year.

**New gTLD Update**

- The General Availability phase for .rio, .whoswho, .coach, .legal, .memorial, .money start this week.
- Top 5 Fastest Growing gTLDs: 1. .xyz, 2. .work, 3. .club, 4. .website, and 5. .wang.
- Top 5 Fastest Growing IDNs: 1. .москва (moscow), 2. .포트 (site), 3. .我爱你 (i love you), 4. .公司 (business organization), and 5. .网络 (network).
- Top 5 Fastest Growing City TLDs: 1. .nyc, 2. .london, 3. .москва (moscow), 4. .tokyo, and 5. .sydney.

**Pharmaceuticals**

- A study by a Timothy Libert, a doctoral student at the University of Pennsylvania, has found that nine out of ten visits to health-related web pages result in data being leaked to third parties like Google, Facebook and Experian.

- As they move to exchange patient information with hospitals and other health care partners, doctors are suffering sticker shock: The vendors of the health care software want thousands of dollars to unlock the data so they can be shared. It may take an act of Congress to provide relief. The fees are thwarting the goals of the $30 billion federal push to get doctors and hospitals to digitize health records. The exorbitant prices to transmit and receive data, providers and IT specialists say, can amount to billions a year. And the electronic health record industry is increasingly reliant on this revenue.

- Gilead Sciences is avoiding billions of dollars in U.S. taxes by booking profits overseas, Bloomberg News says. The drug maker reported foreign income before taxes of $8.2 billion for 2014, earning more in non-U.S. profits than it recorded in non-U.S. sales. The data released in a securities filing suggest that Gilead is taking advantage of U.S. rules that let companies shift valuable intellectual property to low-tax countries.

- Acting on a previous threat, the Japanese government has suspended Novartis pharma operations in the country for breaching adverse effects reporting rules.

- AstraZeneca will pay $7.9 million to settle a lawsuit alleging it paid a pharmacy benefit manager to include its blockbuster heartburn drug Nexium on some formularies at the exclusion of other heartburn medications.

- A team of scientists at the Los Alamos National Laboratory in New Mexico are using the new Biosurveillance Gateway Web site to map epidemics in order better to understand and prevent deadly diseases. The gateway will track outbreaks of ebola, measles, and other diseases, beginning with patient zero. It is the latest development in the field of biosurveillance, the study of how the emergence and spread of diseases can be plotted, understood, and stopped.

**Retail**

- Chico’s FAS Inc. unveiled plans Thursday to cut its capital spending, accelerate stores closures and cut jobs as the women’s specialty retailer seeks to shore up its finances. The Wall Street Journal reported earlier this week that private-equity firm Sycamore Partners had abandoned its attempt to take Chico’s private after failing to line up financing for the deal on acceptable terms. Chico’s said Thursday that it plans to close 120 stores through 2017, including 35 in its newly-started fiscal year. As a result of the realignment of its business, Chico’s said it has eliminated 240 existing positions, or about 12% of its headquarters and field management employee base.
When it comes to data breaches, retailers are one of the biggest targets these days, and now we have some detail on the costs around one of the more high-profile attacks. Target Thursday said that it has booked $162 million in expenses across 2013 and 2014 related to its data breach, in which hackers broke into the company's network to access credit card information and other customer data, affecting some 70 million customers.

Japanese retail sales fell 2.0% in January making it the first decline in seven months due to bad weather and continued decline in real incomes.

After Walmart’s decision to increase its minimum wage more retailers are following suit. This week TJX Cos., announced that its hourly U.S. workers' wages will increase to at least $9 this year and $10 in 2016.

Supermarket chain Aldi plans to open 450 new stores in Texas as part of a five-year plan to grow the chain nationwide.

Longshore and Shipping News reported that the ports of Los Angeles and Long Beach can begin working together to address congestion after U.S. Federal Maritime commissioners on Thursday unanimously approved an amendment this week allowing the two largest U.S. container ports to work together. The amendment clarifies the roughly two-year-old discussion agreement to allow Los Angeles and Long Beach to collaborate on issues including rail operations, chassis supply and storage, vessels calls, truck turn times and terminal operations. Both ports are rushing to reduce months of backlogged cargo, resulting from prolonged labor negotiations, strong volume, chassis dislocation and shipping alliances’ intensified cargo discharges.

The New York Times reported that Apple has been ordered to pay $532.9 million after a federal jury found its iTunes software infringed on three patents owned by Smartflash, a patent licensing company based in Texas. After deliberating for eight hours in the U.S. District Court for the Eastern District of Texas, the jury said that Apple not only had used the Smartflash patents without permission but also had done so willfully.

Slate reported that Barnes & Noble plans to spin off its college bookstores unit into Barnes & Noble Education, a separate publicly traded company this summer. The college bookstores spinoff will take the place of the Nook business separation that Barnes & Noble had been planning since last June.

Pittsburgh Business Times reported that O'Hara-based Giant Eagle, Inc., the region's dominant grocer, is shutting down its Good Cents Grocery + More chain, a discount-oriented grocery business it opened in the wake of Bottom Dollar entering the Pittsburgh market. The company will close all eight Good Cents stores it opened in western Pennsylvania and northeast Ohio.

Users with accounts at Toys “R” Us are informed by the company that a hard password reset procedure has been initiated for their accounts as a result of attempts from a third party to gain unauthorized access. The decision comes not because the toys retailer’s computer network has fallen victim to a cyber-attack, but because a different company was compromised and the cybercriminals used those credentials to log into Toys “R” Us accounts.

Technology

A new targeted phishing campaign has been observed by security researchers to focus on high level security professionals in technical companies, such as CTOs. Researchers at Talos, Cisco’s security intelligence and research group, observed on Tuesday the deployment of the malicious campaign, which delivered emails with subjects related to different payment details and federal taxes.

Ericsson AB said Friday it is suing Apple Inc. for infringing technology patents it says
are critical to many aspects of the U.S. tech giant’s popular mobile devices such as iPhones and iPads.

- TalkTalk, the fourth largest internet-service provider in the U.K., said customer information was accessed after a breach at a third-party company.

- Lenovo’s technological woes are continuing. The personal-computer maker said a cyberattack had taken down its website on Thursday, a week after the company apologized for preloading software on some of its laptops that made customers more vulnerable to hacking.

- Chinese Internet companies have deleted tens of thousands of user accounts as the country prepares to enforce new registration rules that will further cement government control over online discourse.

- CloudFlare has deployed a new level of encryption. The form of encryption, a relatively new transport layer cipher suite known as ChaCha20-Poly1305, has largely been used by Google until now. The algorithm is based on a combination of two other ciphers. Researchers have uncovered evidence suggesting the critical weakness may have been exploited against real people visiting real sites, including Gmail, Amazon, eBay, Twitter, and Gpg4Win.org, to name just a few.

- Superfish and other software containing the same HTTPS-breaking code library may have posed more than a merely theoretical danger to Internet users.

- Attackers took complete control of the company’s valuable Lenovo.com domain name, a coup that allowed them to intercept the PC maker’s e-mail and impersonate its Web pages as a result of the preinstalled Superfish malware.

---

**Telecommunications**

- FCC adopts net-neutrality rule backed by Obama for Internet. The decision means Web traffic for all users will be treated equally, and e-commerce giant Amazon favors the ruling, but opponents say they will fight in court.

- FairPoint Communications has made yet another step forward with its labor unions, announcing that after three days of voting, the International Brotherhood of Electrical Workers (IBEW) and the Communications Workers of America (CWA) have ratified tentative agreements with the telco.

---

**Defense**

- The U.S. Attorney’s Office says that there are no signs of a data breach caused by the theft of five laptop computers from U.S. Central Command sometime in April 2013. “There is no indication of a data breach at this point,” said spokesman William Daniels. “As cases proceed, we always remain open to new information and evidence. However, at this point, the indictment only alleges theft of government computers.”

- President Obama Wednesday directed the Director of National Intelligence (DNI) to establish the Cyber Threat Intelligence Integration Center (CTIIC). The CTIIC will be a national intelligence center focused on “connecting the dots” regarding foreign cyber threats to the nation and cyber incidents affecting U.S. national interests, and on providing all-source analysis of threats to U.S. policymakers. The CTIIC will also assist relevant departments and agencies in their efforts to identify, investigate, and mitigate those threats.
DARPA announced the Communicating with Computers program which aims to develop technology to turn computers into good communicators. DARPA states that CWC aims to accelerate progress toward two-way communication between people and computers in which the machine is more than merely a receiver of commands and in which a full range of natural modes is tapped, including potentially language, gesture and facial or other expressions.

FireEye reports that nearly 80% of phishing emails used in attacks investigated last year used IT and security-related topics, or impersonation of those departments or antivirus vendors in order to lure their victims into opening malware-laden attachments and links. FireEye points to the so-called Sandworm nation-state group's use of the BlackEnergy Trojan as a key example of this shift. Sandworm, which has ties to Russia, has targeted victims in Ukraine with BlackEnergy, as well as against ICS/SCADA networks.

Law Enforcement

- The FBI is offering some serious cash for information leading to the arrest of the bureau’s most wanted cyber criminal, Evgeniy Mikhailovich Bogachev, 31, is accused of hacking 1 million computers in the U.S. and internationally. Newsweek reports that the FBI is offering $3 million for information on capturing Bogachev, who is accused of collecting personal and bank information by installing a malware onto victims’ computers. A Pennsylvania court indicted Bogachev on charges of conspiracy, computer fraud, wire fraud, bank fraud and money laundering in May 2014. Authorities said his last known location was the Russian town of Anapa on the north coast of the Black Sea.

- Servando “La Tuta” Gomez, a former school teacher who became one of Mexico’s most-wanted drug lords as head of the Knights Templar cartel, was captured early Friday by federal police as he tried to sneak out of a house in Morelia, the capital of the western state of Michoacan. He was arrested along with eight bodyguards and associates toting a grenade launcher, three grenades, a machine pistol and assault rifles.

- ISIS has attracted supporters online who, while they don’t participate in attacks or killings, endorse the group’s actions and proliferate its message but the US Justice Department said on Monday that they are willing to indict people who assist ISIS with its use and production of social media. The announcement raises questions about where the government would draw the line between support for a terrorist group and legally protected free speech. Provocative tweets, Facebook posts, and grisly online beheading videos have all been key parts of ISIS’s recruitment and propaganda strategy, and has become one of the hardest elements of the terror group’s rise for U.S. national security agencies and technology companies to combat.

- Reversing its own earlier decision that the false-arrest lawsuit could proceed, the 2nd U.S. Circuit Court of Appeals in Manhattan said in a ruling Monday evening that police made valid arrests of 700 protesters in a “confused and boisterous situation” during an Occupy Wall Street march on the Brooklyn Bridge that spotlighted the anti-financial-inequality movement in its early days. Police said the protesters, who didn’t have a permit, spilled onto the roadway despite warnings to stay on a pedestrian path. Demonstrators said that many didn’t hear a warning and that they thought police had decided to let them onto the road, especially since some officers who initially blocked them turned around and walked ahead of them. The appeals court said that “the failure of a thin line of police officers to physically impede a large group” of marchers doesn’t convey “an invitation to ‘go ahead.’”

- The Justice Department is preparing to release a highly critical report of police in Ferguson, accusing them of making discriminatory traffic stops and creating an environment that bred animosity among African Americans, The New York Times reports. The report, which could be released as early as this week, says Ferguson
police disproportionately ticketed and arrested African Americans, while also relying on them for fines to help balance the budget. The report follows the police shooting death of Michael Brown in August, which led to months of protests. But the Justice Department does not plan to charge the officer, Darren Wilson, following a civil rights investigation.