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

• Mounting witness accounts confirm that the Ghani oil field in Libya was attacked and seized by ISIS fighters in accordance with the textbook published last year by an Al Qaida handbook on the topic. This is the most recent oilfield taken by this method.

Agribusiness

• Ten French dairy firms have been fined more than €190m (£136m) for running a cartel to fix prices. France's competition watchdog has ruled the companies were secretly rigging the market for supermarket own-label yoghurt, soft cheese and desserts between 2006 and 2012.
Insurance/Healthcare

- Data breach notification letters about the Anthem breach are not being sent out in timely enough fashion, according to Senate health committee leaders. Senate health committee Chairman Lamar Alexander and Ranking Member Patty Murray wrote a letter to Anthem President and CEO Joseph Swedish, calling for notification letters to be sent to all 78.8 million potentially affected individuals. The Anthem data breach was discovered on Jan. 29, 2015, but the company waited until Feb. 4, 2015 to make a public announcement. The databases were potentially accessed as early as April 2014, the lawmakers wrote, which means personal data could have been in the wrong hands for some time. More than 50 million Americans have yet to receive a data breach notification letter, according to the duo. These individuals have not officially been told that their personal information was potentially exposed and have not been given information on identity protection services.

Financial Services

- Hackers may have attacked a leading health insurance provider using the same methods employed in the massive data breach incident disclosed last month by another major health insurer, suggesting that a single group may be behind both breaches. Customer data, including bank account and clinical data going back to 2002, may have been compromised in the attack, affecting 11 million people.

Global Intelligence

- Bad news continued the week after millions marched against government corruption, their anger focused primarily on the President and her Worker's Party. On Wednesday her approval rating fell to 13 percent. The number of politicians charged in the Petrobras corruption scandal is now over 50 and includes the Worker's Party Treasurer and the Presidents of both the Senate and Chamber of Deputies. Compounding her problems is the prospect that the economy could shrink in 2015 for the second consecutive year, the first such contraction that severe since the onset of the Great Depression in 1929 and 1930.

Legal and Regulations

- Senate Democrats are divided over the scope of intellectual property reform in legislation that would curb "patent trolls," The Hill reports. Among the sticking points is a fee-shifting provision that would require the loser in patent suits to cover legal fees.

Pharmaceuticals

- Health care provider Premera Blue Cross said on Tuesday that the identifying, financial, and medical information for millions of customers could have been revealed in a cyberattack. The attack potentially affects 11 million customers. About 6 million of those live in Washington state, where some customers are employees at companies like Amazon and Microsoft. Premera said that the e-mail addresses, bank information, and social security numbers for business partners may have also been affected in the breach.

Retail

- Target has agreed to pay $10 million to settle a class-action lawsuit stemming from a massive data breach that compromised the information of up to 40 million shoppers during the 2013 holiday season. Target will pay affected shoppers up to $10,000 each in damages.

Technology

- Facebook, one of the most popular social networks in Russia, reported that content restriction requests from the Russian government increased nearly two-fold during the second half of 2014. In a new installment of their Global Government Requests Report, spanning a period from July 2014 to December 2014, Facebook reported only two government requests for user account data in Russia, and said it did not fulfill any
of them. In contrast, Facebook received no government requests for Russian users’ data during the first half of 2014.

**Telecommunications**

- FCC Chairman Tom Wheeler’s new net neutrality rules are now facing yet another investigation by the FCC’s Inspector General David Hunt, who is also looking into whether the Obama administration improperly influenced the agency’s development of the net neutrality rules, according to reports.

**Defense**

- APT Rocket Kitten, who may have ties to Iran has breached the systems of several organizations in Israel and Europe. Rocket Kitten conducted two campaigns: GHOLE malware distribution, and operation "Woolen-GoldFish," which indicates a state-sponsored campaign. The threat group is “particularly interested in the defense industry, government entities, the IT sector, and academic organizations.” The attack vector reported is spear-phishing.

**Law Enforcement**

- Justice Department attorneys are under scrutiny after a federal judge said they may have misled him about when President Obama’s immigration plans were implemented. The Associated Press reports that U.S. District Judge Andrew Hanen, who has blocked President Obama’s immigration executive action, hinted that sanctions could be forthcoming if he was misled about when the administration launched the controversial immigration plans.

**Energy**

- Employees in the shale oil industry in Jordan protested what they describe as “surprise layoffs.”

- Mounting witness accounts confirm that the Ghani oil field in Libya was attacked and seized by ISIS fighters in accordance with the textbook published last year by an Al Qaida handbook on the topic. This is the most recent oilfield taken by this method.

- An attack in Tunisia’s Bardo Museum is being compared to the Charlie Hebdo attack in France. ISIS has claimed responsibility.

- The Sierra Club is planning a Day of Action against several utilities in Ohio, for efforts to make coal-fired power plants more economically feasible. The Day of Action is planned for April 13.

- The group, We Are Cove Point interrupted a FERC meeting in DC. According to the members, the FERC is stalling on reviewing Dominion Energy’s fraudulent permit and meanwhile construction continues. The group delivered a petition signed by nearly 20,000 people calling on FERC to do its job.

- Florida State University students, climate activists and representatives of a whistle-blower group for environmental employees covered their mouths with tape marked “climate change.” While they delivered a public records request for Florida Governor Rick Scott’s Office to disclose all correspondence between Scott and the Department of Environmental Protection. They also submitted a petition they said was signed by more than 38,000 people and which calls on the DEP Inspector General to investigate whether the ban on using the term “Climate Change” really exists. The group said it was acting in the spirit of this week’s Sunshine Week, a national effort by the media, watchdog groups and individuals to improve government transparency.

- The Obama administration is setting new standards for the controversial hydraulic fracturing process, the first major federal effort to crack down on the practice that has
largely been behind the nation’s oil and natural gas boom. The long-awaited rules from
the Interior Department’s Bureau of Land Management (BLM) are meant, in part, to
ease public fears about a practice that involves pumping fluids miles underground to
extract oil and gas from small pockets in rock. The rules announced Friday set
standards for well construction to minimize the risk of groundwater or other
contamination, strict requirements for disposal of the fluid that flows back out of the
well and a mandate to publicly disclose the chemicals drillers use in them. In addition,
disposal fluid must be stored in covered, above-ground tanks.

Canada’s energy regulator is investigating up to a dozen new allegations of natural gas
pipeline safety-code violations at TransCanada Corp, according to documents
reviewed by Reuters. The regulator, the National Energy Board (NEB), and the
company confirmed an investigation is under way but offered few details of the
allegations. It marks the second time in recent years the regulator has probed safety
practices at Canada’s second-largest pipeline company following complaints by a
whistleblower. Documents reviewed by Reuters showed the allegations include faulty
or delayed repairs, sloppy welding work and a failure to report key issues to the
regulator. TransCanada declined to provide details about the allegations, but noted
someone previously raised them within the company, prompting an internal
investigation that is continuing.

A Navajo advocacy group has asked a federal judge to halt hydraulic fracking permits
in the San Juan Basin of New Mexico, claiming that drilling threatens a historic
UNESCO heritage site considered sacred by Navajo, Hopi and Pueblo peoples. Diné
Citizens Against Ruining Our Environment and three other groups have sued the US
Bureau of Land Management (BLM) and US Department of Interior, calling on a
federal judge to vacate the 130 fracking permits issued by the BLM and enjoin fracking
activity in the Mancos Shale of the San Juan Basin until the BLM adheres to the
National Environmental Policy Act and the National Historic Preservation Act,
according to Courthouse News. The 4,600-square-mile San Juan Basin of New
Mexico’s Four Corners region is home to Chaco Culture National Historical Park, which
includes the Anasazi ruins and other archeological remains of structures that were
among North America’s largest around 1,000 years ago.

Agribusiness

Texas legislators have proposed GMO-labeling legislation in the State House of
Representatives. The bill HB3499 would mandate the labeling of products containing
GMO’s in Texas.

On March 17, Commondreams.org reports that San Diego filed a lawsuit this week
against Monsanto for polluting it’s bay with carcinogenic chemicals that have been
banned in the US for over 30 years, namely Polychlorinated Biphenyls (PCBs). The
suit was filed by the City of San Diego and San Diego Unified Port District.

On March 19, Consumer Reports published a report on measured levels of pesticide
residue on produce. The report does not list specific companies involved in the
manufacture and use of synthetic pesticides, though it does recommend ways of
avoiding pesticides when possible.

In the ongoing court battles over existing legislation in Mexico banning the cultivation
of GM maize, activist groups are celebrating four court decisions favoring the
anti-GMO movement. Despite these recent losses, transnational seed companies such
as Monsanto and Syngenta are continuing to seek appeals.

The low pathogenic H7N3 avian influenza virus was confirmed in a commercial flock of
6,100 turkeys in California, said the World Organization for Animal Health in a notice
on its website. The USDA also identified a strain of highly contagious avian influenza
in a poultry flock in Leavenworth County, Kansas, “the latest flare-up in a multi-state
outbreak threatening U.S. poultry producers.”
• The United States and New Zealand asked the World Trade Organization to rule that Indonesia unfairly restricts imports of fruits, vegetables and animal products, based on regulations imposed in 2012.

• Monsanto, the giant seed company, settled lawsuits fielded by wheat growers in seven states over the 2013 discovery of a GMO variety growing in the wild in eastern Oregon. Monsanto will donate $50,000 apiece to agriculture schools at land-grant universities in Missouri, Illinois, Kansas, Texas, Louisiana, Oklahoma and Mississippi.

• Ten French dairy firms have been fined more than €190m (£136m) for running a cartel to fix prices. France’s competition watchdog has ruled the companies were secretly rigging the market for supermarket own-label yoghurt, soft cheese and desserts between 2006 and 2012.

• About 24,000 chickens were in two chicken houses that caught fire near Puckett, Miss. Tuesday morning. Thousands of chickens perished and the structures were destroyed. The owner of the chicken farm, Van Latham, said about 22,000 chickens were killed. Koch Foods owns the chickens. Authorities are investigating the cause of the fire.

---

**Insurance/Healthcare**

• Health data encryption is becoming an increasingly important issue, especially in the wake of large scale data breaches like Anthem, Inc. and Premera Blue Cross. The HIPAA Omnibus Rule improved patient privacy protections, gave individuals new rights to their health information, and strengthened the government’s ability to enforce the law. However, health data encryption is considered an “addressable” aspect rather than a “required” part of HIPAA.

• More than $27.8 billion has been returned to the Medicare Trust Fund over the life of the Health Care Fraud and Abuse Control (HCFAC) Program, Attorney General Eric Holder and HHS Secretary Sylvia M. Burwell announced Thursday. The government’s health care fraud prevention and enforcement efforts recovered $3.3 billion in taxpayer dollars in Fiscal Year (FY) 2014 from individuals and companies that attempted to defraud federal health programs, including programs serving seniors, persons with disabilities or those with low incomes. For every dollar spent on health care-related fraud and abuse investigations in the last three years, the administration recovered $7.70. This is about $2 higher than the average return on investment in the HCFAC program since it was created in 1997. It is also the third-highest return on investment in the life of the program.

• Data breach notification letters about the Anthem breach are not being sent out in timely enough fashion, according to Senate health committee leaders. Senate health committee Chairman Lamar Alexander and Ranking Member Patty Murray wrote a letter to Anthem President and CEO Joseph Swedish, calling for notification letters to be sent to all 78.8 million potentially affected individuals. The Anthem data breach was discovered on Jan. 29, 2015, but the company waited until Feb. 4, 2015 to make a public announcement. The databases were potentially accessed as early as April 2014, the lawmakers wrote, which means personal data could have been in the wrong hands for some time. More than 50 million Americans have yet to receive a data breach notification letter, according to the duo. These individuals have not officially been told that their personal information was potentially exposed and have not been given information on identity protection services.

• The Department of Health & Human Services (HHS) Office for Civil Rights (OCR) Director Jocelyn Samuels still does not have a set date for when the next round of HIPAA audits will take place. Samuels spoke earlier this week at the 23rd National HIPAA Summit in Washington, D.C., and explained that the OCR has still not finalized the audit procedures. This round of HIPAA audits had originally been scheduled for the fall of 2014, but OCR health information privacy senior advisor Linda Sanches said at the time that the audits were delayed so new technology could be properly
Premera Blue Cross announced this week that it was the “target of a sophisticated cyber attack,” leading to a health data breach that could potentially affect 11 million individuals. The Premera health data breach was discovered by the company on Jan. 29, 2015, and the initial attack occurred on May 5, 2014. Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and the health insurer’s affiliate brands Vivacity and Connession Insurance Solutions, Inc. are all potentially affected. Moreover, members of other Blue Cross Blue Shield plans who sought treatment in Washington or Alaska were also affected by the cyber attack. Applicants and members’ names, dates of birth, email addresses, addresses, telephone numbers, Social Security numbers, member identification numbers, bank account information, and claims information, including clinical information, were all potentially exposed.

Better health IT policies, including national interoperability standards, are essential for the US healthcare industry as it continues to rely on health IT, according to the American Hospital Association (AHA). In a letter to the US Senate Committee on Health, Education, Labor and Pensions, the AHA said that the importance of a strong health IT infrastructure is becoming more necessary. Moreover, shared health information will give clinicians and patients the data they need to promote health and make informed treatment decisions.

A 2014 IT security audit by the US Office of the Inspector General’s (OIG) Office of Personnel Management (OPM) warned Premera Blue Cross that certain security aspects of its information systems were not adequate. Specifically, OPM made suggestions for improvement in several areas, including access controls, network security, and configuration management. The November 2014 report was an audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) at Premera. The investigation took place in January and February 2014. This was the first audit on Premera security controls, and the report stated that all Premera personnel “were helpful and open to ideas and suggestions.” However, the report was filed not long before it was discovered that cyber attackers broke through Premera’s system and gained access to approximately 11 million individuals’ information.

Rep. John Tobia has proposed a bill that reveals what many believe is the follow-up to PIP and sinkholes as the next Great Florida Consumer Scam. The Melbourne Beach Republican’s bill attacks insurance-claims abuses in something called “assignment of benefits” (AOB). AOB is a legal process within insurance policies intended to make sure a vendor, or repairman, gets paid quickly after work is done -- for example, a contractor repairing home damage without requiring the policyholder to be involved in the payment process. In this scheme, AOBs are being used to inflate claims and file costly lawsuits against insurers.

New Jersey drivers who lie about where they garage and drive their vehicles to illicitly lower their auto premiums are a big step closer to facing stiff new penalties for being caught, according to the Coalition Against Insurance Fraud. A bill making it a crime of insurance fraud to falsely register vehicles in other states cleared the legislature yesterday and heads to the governor for his potential signature. The Coalition is urging governor Chris Christie to sign and enact the bill into law.
financial support to New York charter schools. The same group also held a protest outside the same hedge fund manager’s home residence in New York City on March 21. Previously, the anti-hedge fund activist group conducted a protest action outside the Greenwich, CT home residence of a separate hedge fund manager on March 14 for similar reasons.

- An array of allied organizations held a protest at the World Bank in Washington, DC on March 19 to demand that the international bank stop the lawsuit against El Salvador that could force the country to “shell out hundreds of millions of dollars” for trying to protect its major river system from pollution from cyanide-based gold mining.

- Housing activists swarmed the Wayne County commissioners meeting in Detroit, MI on March 19, demanding that the county commissioners back the call for a Declaration of a State of Emergency in the county due to the amount of tax foreclosures in the area. The activist also launched an online petition demanding a moratorium on tax foreclosures.

- A 'March Against Capitalism' action occurred on March 21 in downtown Los Angeles, CA.

- Protests occurred at the global offices of an American multinational private equity and investment firm on March 17 in solidarity with Spanish housing activists demanding that the firm stop speculating on housing and ultimately causing foreclosures and evictions. Most notably protest actions occurred in New York City, San Francisco, London, and several Spanish cities.

- Activists held a protest on March 16 at the New York State Capitol Building in Albany, NY demanding a stop to Governor Cuomo’s proposed budget that allegedly serves billionaires, hedge fund managers, and multinational corporations instead of the people of New York.

- A protest against the Transatlantic Trade and Investment Partnership (TTIP) will occur in Dublin, Ireland on Friday, March 27. The protest corresponds with the visit of European Commissioner of Trade to Dublin.

- Activists in Dublin, Ireland will conduct a mass protest march on April 15, starting at the Central Bank of Ireland on Dame Street and heading to the Irish Parliament (Dail) to raise awareness for the homeless situation. Participants are also planning a sleep-in outside the Dail on the night of the protest/march.

- A protest against austerity measures employed by the Canadian Government will occur in Montreal, Canada on Monday, March 30.

**Information Security Risk**

- The National Credit Union Administration, a U.S. federal banking regulatory agency, issued a warning about a new phishing campaign that aims to con consumers into disclosing personal and financial details by feigning to be a request from the regulator. The agency recently announced that it received reports of an online phishing scam that uses a website with a logo and a design similar to the agency’s own site in an attempt to convince unwary customers to provide information or send money.

- Microsoft issued a warning that a fraudulent SSL digital certificate has been issued in the name of a Finnish version of its Windows Live service. Although the company says it has revoked the certificate, security experts warn that older software may continue to “trust” the known bad certificate for months or even years, and that attackers could use it to trick users into running malware.

- A total of 1,228 Android apps that have been downloaded 6.3 billion times from the Google Play store are still vulnerable to the FREAK bug. According to researchers, as of March 4, both of the latest Android and iOS platforms are vulnerable to the security issue. As FREAK is both a platform vulnerability and an app vulnerability, even after Google and Apple issued patches, apps may still be vulnerable when connecting to servers that accept RSA_EXPORT cipher suites.
Hackers may have attacked a leading health insurance provider using the same methods employed in the massive data breach incident disclosed last month by another major health insurer, suggesting that a single group may be behind both breaches. Customer data, including bank account and clinical data going back to 2002, may have been compromised in the attack, affecting 11 million people.

Some computer systems and servers at a not-for-profit health care organization headquartered in Milwaukee, WI were infected with malware designed to capture log-in data entered on certain websites mostly providing financial services. The incident was discovered on January 27, 2015, and the organization took action towards removing the malicious files from its computer network. The hospital said patient information was not exposed and that only caregivers are at risk.

Federal authorities investigating the data breach at the largest U.S. bank are confident that a criminal case will be filed against the hackers in the coming months. The NYC-based bank said last October that names, addresses, phone numbers and email addresses of about 83 million customers were exposed in the attack, making it one of the biggest data breaches in history. Law enforcement officials believe that several of the suspects are "gettable," meaning that they live in a country with which the United States has an extradition treaty.

A piece of Android banking malware known as Trojan.Spy.FakeBank.ir is targeting Iranian online banking users and can steal two-factor verification codes. Once installed on a victim's phone, the app monitors SMS activity for incoming verification messages from the Iranian bank it seeks to imitate. When one arrives, it copies the information into another message and sends it out via SMS, presumably to the app's operator. Though the app targets Iranian Android users, its command and control servers appear to be located in Latvia. Interestingly, the app only captures the two-factor authentication texts and not the victim's main username and password. Researchers believe this is a case in which the mobile Trojans is working in conjunction with desktop Trojans to steal victims' banking information.

Cybercriminals are using a software tool called Antidetect to evade fraud detection schemes employed by many banking websites. Antidetect allows users to very quickly and easily change components of the their system to avoid browser fingerprinting, including the browser type (Safari, IE, Chrome, etc.), version, language, user agent, Adobe Flash version, number and type of other plugins, as well as operating system settings such as OS and processor type, time zone and screen resolution.

A leading U.S. financial institution informed its customers on March 16th that their personal information had been accessed and distributed by a former employee to a third-party. The employee was still working for the bank at the time of the event, and following the disclosure of the data to the unauthorized entity, fraudulent charges were recorded for the accounts of the impacted customers. An investigation is ongoing to determine how the data was accessed and leaked.

Legal, Litigation, Regulatory Risk

A bipartisan group of Senators are fighting back against a "budgetary gimmick" that allows the federal government to use funds raised from guaranteed GSE fees to cover federal spending. An industry insider lamented that guaranteed fees should be used to protect taxpayers from risk, but some want to increase these fees simply to create "a piggy bank for Congress."

An article reported that Argentina will not allow a leading U.S. bank to exit its local custody business, setting up a possible showdown between the leftist government and the banking giant over sovereign debt payments. The bank has found itself at the center of a bitter court battle between Argentina and a group of New York-based hedge funds that were awarded full payment on their defaulted sovereign bonds by a U.S. District Judge. The Judge barred Argentina from servicing other debt and blocked financial institutions from processing payments, including an upcoming March 31 payment, until it paid the funds. But Argentina, arguing that the rulings impinge on its national sovereignty, has threatened to revoke the bank's license in the country if it
does not process the next payment.

- A leading Switzerland-based multinational financial services holding company will pay $10 million in cash and provide $6.25 million worth of advisory work to one of the world's largest producers of copper and gold based in Phoenix, Arizona to settle allegations that the bank contributed to the natural resources company having overpaid significantly for two oil and gas companies.

- The Securities and Exchange Commission approved a shareholder proposal, filed by a consumer-rights advocacy group, that seeks to break up a leading “too-big-to-fail” U.S. investment bank. While the nonbinding referendum is unlikely to lead to the bank’s dismantlement, the proposal marks the first time the SEC has supported a shareholder vote on splitting up a major bank.

**Operational Risk**

- A new survey said that businesses fear losing clients as a result of DDoS attacks. The survey revealed that 26 per cent of companies thought the problems caused by such attacks were long-term, meaning they could lose current or prospective clients as a result. 23 per cent said they were concerned a DDoS attack would cause reputational issues, while 19 per cent thought the risk of losing current customers who were not able to access services as a result of an outage was the biggest threat to business. The research revealed that only 37 per cent of the companies surveyed had measures already in place to protect against DDoS attacks.

- A removable storage drive containing social security numbers (SSN) belonging to employees of a leading national restaurant management company was lost by someone working for a third-party vendor in charge with improving payroll services for the company. The incident occurred while the payroll consultant was travelling. Apart from the SSNs, the company said in a letter disclosing the incident that the drive included the details for the W-2 IRS form, where employers are required to provide data on employees’ names, wages and tax information.

- According to figures released last week in the Netherlands, the damage done by fraud during payment transactions in the country decreased significantly last year from 33.3 million euros in 2013 to 17.3 million euros in 2014. The report also noted that there was a considerable decrease in debit card skimming last year as well. The damage caused by skimming fell from 6.8 million euros in 2013 to less than 1.3 million euros last year, a decrease of 82 percent. Skimming has become unattractive to fraudsters due to the introduction of the EMV payment chip, “geo-blocking” pin codes outside Europe and additional anti-skimming measures. Losses due to internet banking fraud decreased by 51 percent, from 9.6 million euros in 2013 to 4.7 million euros last year. Damages caused by malware decreased as well by 90 percent to less than 500 thousand euros. The report said that the downward trend in banking fraud is due to the fact that Dutch banks are getting better and better at automatically detecting and preventing malware. The most damage was caused by phishing which accounted for 3.9 million euros last year, a figure that’s still lower that the 4.7 million euros in 2013.

- Germany, France and Italy followed Britain last week in announcing that they plan to join a proposed Chinese-led Asian regional bank, swinging Europe's biggest economic powers behind a project that is viewed with concern in Washington. Britain two weeks ago became the first major Western country to seek membership in the Asian Infrastructure Investment Bank. Last week's announcement brought three more members of the Group of Seven industrial powers on board. China proposed the bank in 2013 to finance construction of roads and other infrastructure. It has pledged to put up most of its initial $50 billion in capital. Twenty-one other governments including India, New Zealand and Thailand have said they want to join, but the U.S. and close allies Japan, South Korea and Australia have not. The United States has expressed concern that the new bank will allow looser lending standards for the environment, labor rights and financial transparency, undercutting the World Bank and International Monetary Fund. The Europeans appeared at pains to counter those concerns.

- An article reported that legislators have future liquid concerns about the GSEs for
housing and fear that they may need more taxpayer support. These concerns are the result of profits and capital cushions reduction in recent quarters. The article said that the GSEs have signed an agreement to reduce their financial cushions until 2018 and all their profits are being “Swept” into the treasury departments.

**Reputational Risk**

- An article reported that after 16 banks caved in to White House demands to refund billions in losses to the two GSEs for housing, a leading Japanese bank refuses to succumb to the political pressure. The bank’s U.S. unit won’t give in to the regulators who claim it hoodwinked the toxic GSEs into buying pools of subprime mortgages, like it claimed many other major U.S. banks did in the run-up to the mortgage crisis. The government demands $1 billion in damages. The Japanese bank says it won’t give a dime toward the $18 billion “ransom” the feds already have shaken out of other banks who settled with the Federal Housing Finance Agency. Instead, it will make the government prove it in court.

---

**Global Intelligence**

**Brazil**

- Bad news continued the week after millions marched against government corruption, their anger focused primarily on the President and her Worker’s Party. On Wednesday her approval rating fell to 13 percent. The number of politicians charged in the Petrobras corruption scandal is now over 50 and includes the Worker’s Party Treasurer and the Presidents of both the Senate and Chamber of Deputies. Compounding her problems is the prospect that the economy could shrink in 2015 for the second consecutive year, the first such contraction that severe since the onset of the Great Depression in 1929 and 1930.

**Canada**

- Canadian regulators, the Canadian Radio-television and Telecommunication Commission (CRTC), declared that cable operators in the country must now start unbundling cable channels. According to the CRTC, operators like Rogers, Shaw and Bell must offer a ‘skinny bundle’ of channels for at least $25 a month. Canadian cable TV providers will also be forced to require consumers with a la carte channel choices at ‘reasonable prices.’ This new regulation does not come into effect until December 2016.

**China**

- An article on Freebuf.com contains analysis of a malicious trojan called TROJ_VICEPASS.A. According to the article, TROJ_VICEPASS.A will be disguised as an Adobe Flash update file to lure users to download and install. Once installed, it will attempt to connect to a router, and search for any devices that are connected to the network. After that, it will attempt to log into the connected devices with pre-prepared login credentials to steal sensitive data, sent it to a remote server and uninstalled itself.

- An article on QQ.com discusses a security vulnerability of the USB-C port on the new MacBook. According to the article, the new MacBook with USB-C port is more vulnerable to hacker attacks and powerless to the BadUSB vulnerability.

- An article on Workercn.cn reports that China’s National Computer Virus Emergency Response Center discovered a new variant of Trojan_Generic.AQM. The new variant is able to copy and rename itself to avoid detection by anti-virus softwares. Trojan_Generic.AQM will download additional malwares onto infected devices.

**Malaysia**

- An article on MalaysianInsider.com reports former Gua Musang MP Tengku Razaleigh
Hamzah is questioning the Malaysian government on the face that the Goods and Services Tax collected will be used to pay off the federal government’s debts or for the benefit of the people. The Goods and Services Tax will be in effect on April 1, 2015.

- An article on Freemalaysiatoday.com reports the high number of illegal foreign workers in Malaysia pose a “frightening threat” of tuberculosis, due to almost the half the legal foreign workers testing positive for tuberculosis, while the illegal foreign workers are not tested.

**North America**

- Reuters reported that trade associations representing large U.S. Internet service providers (ISPs) are expected to take the lead in suing the Federal Communications Commission over its new web traffic regulations, according to several people familiar with the plan. Such an approach would allow companies to streamline their litigation efforts and could help firms avoid drawing any fire individually. At least three trade groups are expected to file legal challenges: CTIA-The Wireless Association, the National Cable and Telecommunications Association and the broadband association USTelecom. Other trade groups such as the American Cable Association and the National Association of Manufacturers are weighing whether to participate in litigation.

- Sony confirmed that be launching a Playstation Vue program, the company’s Internet TV services. The platform will initially be launching for PS3 and PS4 users in just three cities: New York, Philadelphia, and Chicago. Unlike Dish’s Sling TV, PlayStation Vue is intended to be a full cable replacement for cord cutters with packages starting at $50/month.

- The New York Post reported that Apple is offering to share data with programming partners to get them on board with its cable-like TV network package. Apple is willing to share details on who its viewers are, what they watch and when they watch it to entice broadcast networks and others to go along with the service.

- DSL Reports reported that Dish Network continues to add channels to its recently released Sling TV Internet video service. It will be adding A&E, History, H2 and Lifetime to its $20 core live TV package, AMC Newtorks and IFC were added to it service earlier in March.

- Google has received an okay from the FCC for broadband drone trial in the Southwest. The FCC approval does not give away technical specifics regarding the project other than the fact that the trials will run from March until September and will take place outside of Albuquerque, NM.

- New research studies from Leichtman Research Group, Inc. found that 81% of households in the US have at least one high definition television (HDTV) set, and about 52% of all households have multiple HDTVs. Five years ago, 46% of US households had at least one HDTV, and 17% of households had more than one HDTV.

**Taiwan**

- An article on Huanqiu.com reports the government of Taiwan will be setting up a new department that solely concentrates on national cyber security, especially combating the frequent attacks launched by China’s Communist Cyber Army.

---

**Legal and Regulations**

- Rep. Adam Schiff of California, the top Democrat on the House Intelligence Committee, said NSA surveillance reform can’t move forward until Congress passes a comprehensive cybersecurity measure, National Journal reports.

- Senate Democrats are divided over the scope of intellectual property reform in legislation that would curb “patent trolls,” The Hill reports. Among the sticking points is
On March 18, in an effort to help employers understand which rules and policies will pass the NLRB's scrutiny, the NLRB's General Counsel issued a 30-page memo intended to clarify any confusion. It's important to keep in mind that the General Counsel's memo does not have the force of law. It is only an indication of the likely position the NLRB will take if an unfair labor practice charge is filed over the rules and policies contained in an employer's handbook. However, employers should expect Board scrutiny of workplace policies to increase following this Report.

**Worldwide**

Given America's record of mass surveillance, can Facebook store data on its European users in US servers? That's the question the European Union's Court of Justice will convene Tuesday to discuss. The EU allows companies to transmit data abroad only if they can ensure "adequate protection" of users' privacy. Should the court rule Facebook cannot ensure those protections, the decision will likely impact other American companies with European users, from Microsoft to Apple. The court has a history of favoring users' privacy. Last year, in a well known decision, it ruled against Google in support of Europe's "right to be forgotten" law, in which Europeans can compel the Internet giant to remove certain personal information from search results.

**Pharmaceuticals**

- As the Evolution black market dissolved all of a sudden recently, its admins making millions of escrow dollars disappear overnight, the owners of alternative dark web drug bazaar Middle Earth scramble to assimilate its customers.

- Several years ago, Novartis agreed to pay $175 million to settle a high-profile gender discrimination lawsuit focused on its U.S. sales operations. Now, the Swiss drugmaker faces a new discrimination fight at its Texas-based Alcon unit. Two former Alcon employees sued Alcon and its parent company for $110 million, alleging that the company pays women less than men, promotes women less than men, and fosters a "boy's club" atmosphere that at best makes women uncomfortable and at worst shuts them out of better opportunities at the company. One of the plaintiffs is asking for class action status, on behalf of other female employees.

- Two female employees of Boston Scientific's neuromodulation business filed a $50 million class-action lawsuit alleging sex discrimination, alleging that the company fosters a culture in which men feel free to harass and discriminate against women.

- Actavis is eliminating more than 400 jobs as part of previously announced plans to consolidate operations following its acquisition last year of Forest Laboratories. Most of the jobs, which were in sales and marketing or various administrative functions, were located in Long Island, N.Y., according to a filing with New York state officials.

- A security breach at one of the third-party vendors of Sacred Heart Health Systems has resulted in the exposure of health and personal information of approximately 14,000 patients. Hackers were able to access patients' names, dates of service, dates of birth, diagnoses and procedures, total charges, and physicians' names, and 40 of the patients Social Security numbers were also compromised, through phishing attack by gaining access to the email account of an employee of the billing vendor.

- An intruder had accessed internal membership information of more than 151,000 patients of an Advantage Dental, a Redmond-based provider that serves low-income patients at more than 30 clinics in Oregon, in late February, announced on Monday. According to the Advantage Dental, there is unauthorized access to patients' names, social security numbers, home addresses, phone numbers, and dates of birth, but treatment details, payment or other financial data were not accessed. A malware obtained a username and password of Advantage employee's computer that allows
access to the membership database, which is separate from the database that contains financial and treatment information.

- Children's National became a victim of a cyber-attack, after its employees responded to phishing emails by hackers believing they were legitimate. The issue came to light on December 26 last year and Children's National believes that any potential unauthorized access of its employees email accounts could have taken place between July 26 and December 26 last year.

Retail

- Target has agreed to pay $10 million to settle a class-action lawsuit stemming from a massive data breach that compromised the information of up to 40 million shoppers during the 2013 holiday season. Target will pay affected shoppers up to $10,000 each in damages.

- Amazon.com Inc. appears to have beaten Google and a handful of others for the .free domain name. A spokesman for the International Corporation of Assigned Names and Numbers, which manages the names and numbers of web addresses and is known as ICANN, wouldn’t confirm that Amazon had won the bidding for the domain name. However, a check of the application status for the domain shows that of the five bids submitted, Amazon’s is the only one not withdrawn.

- Over the last two years, men’s retail sales jumped 4.1% to $101.8 billion, eclipsing the 2.8% rise to $150.1 billion on the female side, according to research firm Euromonitor. By 2017, menswear is expected to climb 8.3% to $110.3 billion, compared with 4.2% to $156.5 billion in women’s. Although women’s clothing still sells more, menswear has been expanding at a faster clip and the expansion is being driven by millennial guys in their 20’s and 30’s.

- WebMD reported that a Los Angeles law that restricts the opening of new fast food restaurants in poor areas has not lowered obesity rates among people who live in those neighborhoods, a new study finds. "The South Los Angeles fast food ban may have symbolic value, but it has had no measurable impact in improving diets or reducing obesity," study author Roland Sturm, a senior economist at RAND Corp., said in a news release from the nonprofit research organization.

- The Detroit Free Press reported that after a point-of-sale system outage at Meijer recently, the company is offering $10 coupons that customers can use Friday or Saturday. The coupon is good for $10 off a $50 purchase on grocery, health and beauty items or general merchandise. Frank J. Guglielmi, senior director of communications for the Grand Rapids-based retailer, said an outage affected the retailer’s ability to process credit cards. He noted it was an internal IT issue.

- The Chicago Tribune reported that Kraft Foods is recalling about 242,000 cases of its macaroni & cheese after eight consumers complained about possible pieces of metal in the well-known blue boxes. It is possible some boxes may contain small pieces of metal, Northfield-based Kraft said Tuesday. The company said no injuries have been reported and apologized to consumers. It is the latest in a string of recalls by the food company over the past several months.

- The Christian Science Monitor reported that McDonald’s workers have filed safety complaints with a regulatory board alleging frequent on-the-job injuries, lacking safety equipment, improper training, and pressure to work at unsafe speeds. The new complaints are part of a larger effort to hold McDonald's legally culpable for the actions of its franchisees.

- The Dallas Morning News reported that cosmetics retailer Mary Kay has filed a lawsuit in federal court against digital coupon giant RetailMeNot, claiming the company is soliciting coupons for the cosmetic company without its consent. Mary Kay says in the suit, filed on Friday in U.S. District Court in Dallas, that it does not provide digital deals,
offers and coupons for publication on RetailMeNot and has not authorized or permitted
the site to list deals, sales or codes using its name or likeness. RetailMeNot has since
prepared a statement claiming it believes to be in compliance with the law, but that the
company is prepared to fight back in the suit.

- The New York Times reported that federal regulators have given Amazon a green light
to begin testing drones, but it will most likely take years before the online retailer can
start delivering packages from the air to peoples’ homes. The Federal Aviation
Administration on Thursday gave Amazon permission to conduct test flights of its
drones outdoors, as long as the company obeys a host of rules like flying below 400
feet and only during daylight hours.

Technology

- Facebook, one of the most popular social networks in Russia, reported that content
restriction requests from the Russian government increased nearly two-fold during the
second half of 2014. In a new installment of their Global Government Requests
Report, spanning a period from July 2014 to December 2014, Facebook reported only
two government requests for user account data in Russia, and said it did not fulfill any
of them. In contrast, Facebook received no government requests for Russian users’
data during the first half of 2014.

- Dridex trojan malware is evading detection by including the AutoClose method.
Traditionally, the malware executes upon opening a document but Dridex has evolve to
execute when the document is closed. The malware payload “listens” for a document to
close event as a trigger to execute.

- Security researchers developed a new BIOS bookit that exploit recently discovered
vulnerabilities. BIOS bookits are a reality despite there is little evidence of BIOS
implants in the wild. The BIOS bookit was mentioned when Snowden disclosed the
catalog of surveillance tools used by the NSA ANT division, these malicious malware
are able to compromise the BIOS of the victim’s machine ensuring persistence and
implementing sophisticated evasion techniques. The BIOS implant survives even is the
OS is re-installed.

- An activist group that monitors the Chinese web, GreatFire, has suffered a DDoS
attack that cost them $30,000 a day. The attack was delivering up to 2.6 billion
requests per hour, started on Thursday, shortly after an article about how the group
used cloud services to circumvent censorship appeared on the Wall Street Journal
website.

- Application-layer bot attacks affects almost every website on a daily basis but are
overlooked by the media. Dark Reading reports that DDoS attacks are only “one
manifestation of sophisticated bot attacks” but because botnets are the source of the
attack they should have more attention. Dark Reading’s author notes that the “real and
far more likely bot threat against your business website comes from low-profile, often
overlooked bots that secretly scan and test for ways to steal business data, content
and intellectual property, or penetrate your defense.”

Telecommunications

- Windstream’s new CEO Tony Thomas has revealed that former CEO Jeff Gardner’s
resignation from the company in December was due to the company’s financial and
operational performance.

- FCC Chairman Tom Wheeler’s new net neutrality rules are now facing yet another
investigation by the FCC’s Inspector General David Hunt, who is also looking into
whether the Obama administration improperly influenced the agency's development of the net neutrality rules, according to reports.

Defense

- The State Department said Tuesday it has reopened Internet service on its unclassified worldwide email network after it was shut down for four days to clean up malware and boost defenses against cyberattacks believed to have started last fall. The State Department shut down its unclassified email system on Friday after malware was detected in November, saying the incident demonstrated that it was among "a growing list of public institutions and private industries facing an increasing number of sophisticated cyber threats." The agency wouldn't confirm published reports that the Russian government was behind the hack, but it stressed that its classified systems weren't affected.

- The Russian government is set to introduce a special procedure for financing the country's defence industry during the current financial crisis, Russian deputy prime minister Dmitry Rogozin told a meeting of defence industry leaders on 18 March.

- The government's efforts to deter computer attacks against the United States are not working and it is time to consider boosting the military's cyber-offensive capability, the head of U.S. Cyber Command told Congress on Thursday.

- APT Rocket Kitten, who may have ties to Iran has breached the systems of several organizations in Israel and Europe. Rocket Kitten conducted two campaigns: GHOLE malware distribution, and operation "Woolen-GoldFish," which indicates a state-sponsored campaign. The threat group is "particularly interested in the defense industry, government entities, the IT sector, and academic organizations." The attack vector reported is spear-phishing.

- NATO allies are scrambling to protect vulnerable Baltic partners from the threat of hybrid warfare, a Russian tactic that officials and experts say is based on deception rather than formal declaration of war. According to James Sherr of Britain's Chatham House think-tank, hybrid warfare is "designed to cripple a state before that state even realizes the conflict has begun." Putin's brand of hybrid warfare also relies on "misinformation, bribery, economic pressure", which are designed to "undermine the nation", according to Latvian Defence Minister Raimonds Vejonis.

Law Enforcement

- Justice Department attorneys are under scrutiny after a federal judge said they may have misled him about when President Obama's immigration plans were implemented. The Associated Press reports that U.S. District Judge Andrew Hanen, who has blocked President Obama's immigration executive action, hinted that sanctions could be forthcoming if he was misled about when the administration launched the controversial immigration plans.

- The FBI directed a local police department to drop criminal charges against a suspect in 2012 to avoid the public finding out about a secret device to track people. The device, called the "Stringray," allows investigators to find suspects by tracking their cell phones. The technology mimics a cell phone tower, tricking the phone into switching over to the "Stringray" while investigators access the location. Judge Patrick H. NeMoyer in Buffalo, NY, has indicated he wants the FBI to turn over details of the secret technology that the bureau was using with Erie Police in Pennsylvania. According to CNN, police used the device to track several criminal suspects, four
A Border Patrol agent told a Senate committee Tuesday that Homeland Security is fudging border statistics to make the border seem safer than it actually is, The Business Insider reports. "I want to be crystal clear – the border is not secure," said border agent Chris Cabrera in prepared testimony before the Senate Homeland Security Committee on Tuesday. "That is not just my opinion or the position of the NBPC," he said, speaking on behalf of the National Border Patrol Council. "Ask any line agent in the field and he or she will tell you that at best we apprehend 35 to 40 percent of the illegal immigrants attempting to cross. This number is even lower for drug smugglers who are much more adept at eluding capture." Cabrera said the number of footprints from immigrants, for example, are severely under counted and that supervisors create incentives for agents to lie.

The FBI is investigating a large cyberattack on the Premera health insurance company after concerns that personal and financial information of nearly 11 million customers has been compromised, ABC News reports. Premera said there's no evidence yet that data was used "inappropriately." The company discovered the "sophisticated attack" nearly seven weeks ago and quickly learned that the hacking began in May 2014. The FBI was immediately notified, the company and bureau said.

A man accused of shooting two police officers last week in Ferguson was not targeting police nor aiming at demonstrators at a late-night protest, his attorney said Monday, countering an earlier police description of the crime. Defense attorney Jerryl Christmas also suggested that St. Louis County police may have used excessive force when arresting the suspected shooter, Jeffrey Williams, saying his client had bruises on his back, shoulders and face and a knot on his head.

A number of police oversight bills introduced in the Colorado Legislature includes a measure that would impose up to $15,000 in civil penalties if a law enforcement officer seizes or destroys a citizen's recording or interferes with someone trying to film them.