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**
- Secretary of State John Kerry is positioning himself as a climate leader for upcoming international meetings. In a speech to the Atlantic Council he attacked forty percent of the world’s electricity source, coal, saying investment in coal power was “simply destructive.” He also said he wanted to “stop government funding” for coal and oil, adding it “made no sense” to invest in high carbon sources of energy. Kerry said the US would target “wasteful fossil fuel subsidies” at upcoming meetings of the G20 and Asia Pacific Economic Cooperation forum, which count the world’s top coal users as members.

**Agribusiness**
In a 40-page report, Oxfam America suggests several steps to improve Feed the Future, an Obama administration initiative that uses public-private partnerships to boost local food production in targeted countries. The program has made “substantial, real and important improvements” in U.S. food security efforts, but “the ambitious agenda embraced by U.S. AID remains a work in progress.”

**Insurance/Healthcare**

- While federal regulators flesh out details of a 10-year roadmap for electronic health record interoperability, which would pave the way for national data exchange, five GOP senators are demanding that more attention be paid to the plans for security and privacy of patient data as it’s shared among healthcare providers.

**Financial Services**

- Both Apple and Microsoft released patches to fix the FREAK vulnerability that could help attackers intercept secured network communications. Discovered earlier this month, FREAK (Factoring attack on RSA-EXPORT Keys) provides a way for an attacker to intercept SSL-encrypted traffic encrypted by SSL (Secure Sockets Layer) as it moves between clients and servers. An attacker could use the flaw to secretly access and even alter communications between two parties.

**Global Intelligence**

- On March 15 over a million Brazilians took to the streets to call for the impeachment of President Dilma over corruption in her party and across the government as the Petrobras corruption scandal continues. Unlike the nationwide protests that occurred in June of 2013 that cut across party lines and socio-economic strata to protest the sad state of public services and infrastructure, Sunday’s protest was a mass mobilization of the half of the electorate that is embarrassed and deeply frustrated at Dilma and the government. Unless Dilma gets directly implicated in the Petrobras scandal it is unlikely that there is any viable basis for her impeachment. Calls by some of the protesters for the military to take over the government will go unheeded by the most professional Army in Latin America content to serve their constitutional role in support of the nation’s civilian leaders.

**Legal and Regulations**

- Last week, the National Institute of Standards and Technology (NIST) released a preliminary discussion draft of its Framework for Cyber-Physical Systems. The goal of this draft: to create an integrated framework of standards that will form the blueprint for the creation of a massive interoperable network of cyber-physical systems (CPS), also known as the “Internet of Things.” In 2014, NIST established the cyber-physical systems public working group (CPS PWG)—an open public forum which includes representatives from government, industry, and academia—to develop the CPS framework. By creating a common framework at an early stage of the Internet of Things, the CPS PWG hopes to ensure the development of a secure, integrated, and interoperable ecosystem of connected devices. The CPS PWG will continue to solicit input as it refines the draft and works to finalize the framework for use in multiple industry sectors.

**Pharmaceuticals**

- In the latest dust up over prescription drug costs, Gilead Sciences and Vertex Pharmaceuticals shareholders will be allowed to vote on resolutions that would require the drug makers to publish reports evaluating the risks of the pricing policies for the medicines.

**Retail**

- NEXTEP Systems, a Troy, Mich.-based vendor of point-of-sale solutions for restaurants, corporate cafeterias, casinos, airports and other food service venues, was recently notified by law enforcement that some of its customer locations have been compromised in a potentially wide-ranging credit card breach.
Technology

- U.S. technology companies need to confront difficult choices amid new bank-security rules in China, as Beijing offers few signs that it will abandon measures that could limit the IT firms’ sales to the big market. Banks faced a Sunday deadline to submit plans to Chinese officials on how they will convert their internal technology into what Beijing considers secure and controllable systems.

Telecommunications

- A Dutch court Wednesday handed a victory to privacy advocates by striking down a data-retention law that gives the government easy access to telecommunication data. The District court of The Hague said the law, which requires telecom providers to collect and store data for as long as 12 months, violates citizens’ right to privacy and the right to protection of personal data. “The judge finds that this violation is not limited to what is strictly necessary,” it said.

Defense

- The Wikimedia Foundation on Tuesday joined with other rights groups to file suit against the US National Security Agency's spying program--in particular, its large-scale search and seizure of internet communications, commonly referred to as upstream surveillance.

Law Enforcement

- The Wall Street Journal reports the Justice Department's newest electronic dragnet--plane-mounted "dirtboxes" that can slurp thousands of cellular phone ID's from the air which was originally developed by the CIA to hunt terrorists in the Middle East is now being used domestically to track American citizens. These dirtboxes are electronic sniffers that mimic cellular tower signals to incite any cellular telephone within range to broadcast its identifying registration information to law enforcement.

Energy

- An oil field rig has exploded in West Texas, killing three workers. Investigator Dusty Kilgore of the Upton County Sheriff's Office said the accident happened Tuesday morning near Rankin, about 40 miles south of Midland. Kilgore says a pulling unit crew was at the site when the explosion happened. The Occupational Safety and Health Administration website describes a pulling unit as a well-servicing outfit.

- In a case scheduled to be heard later this year before the Texas Supreme Court, a group of big energy companies will argue that the City of Houston is breaking Texas law. The big companies -- which include ExxonMobil and ConocoPhillips -- say only the state can legally enforce Texas environmental laws. Lawyers for the industry did not make themselves available for an interview. But in briefs filed with the court, they argue that Houston is going rogue, enforcing state pollution laws because: “Houston disagrees with the TCEQ's enforcement actions.” TCEQ is the Texas Commission on Environmental Quality.

- Upset about Sen. Michael Bennet's support of the Keystone XL pipeline, demonstrators gathered to protest at the senator's 2016 campaign fundraiser kickoff Sunday evening in Denver. Hoisting signs reading, "We don't vote for fossil fuel politicians," protesters chanted as nearly 200 Democrats streamed into Denver's Mile High Station for the event. "Senator Bennet has shown he'll compromise his values for votes," said Russell Mendell of Boulder. "If he continues to do so, we'll find a candidate who values their community." Ryan Denham is a member of the organization 350 Action. He said Bennet's vote would make sense if he were a climate-change skeptic, although Denham says the senator has said he is not. As people began arriving for the event,
some grabbed fliers from protesters while others declined to do so and headed to the entrance. Bennet was taken in through a back door and did not address the demonstrators.

- Inside Climate News has posted an article discussing how scientists have linked an increase in respiratory illnesses with extreme weather conditions caused by climate change. The article reads: Scientists have attributed the frigid temperatures and historic snowfalls to storm tracks that have become stronger and more frequent because of increased greenhouse gas emissions that alter atmospheric conditions. Scientists at the American Thoracic Society who specialize in the treatment of respiratory illnesses are connecting some of their patients’ disorders to climate change.

- Research by Frohlich and others have linked disposal wells and oil and gas extraction to earthquakes in Texas. Most of these earthquakes have been small enough or far enough away from communities that they haven’t caused injuries or damage to infrastructure. But some researchers argue an increase in small tremors ups the odds of a big quake. And while new state regulations make earthquakes a consideration for permitting disposal wells, further research and management could help energy companies develop oil and gas safely.

- Secretary of State John Kerry is positioning himself as a climate leader for upcoming international meetings. In a speech to the Atlantic Council he attacked forty percent of the world’s electricity source, coal, saying investment in coal power was “simply destructive.” He also said he wanted to “stop government funding” for coal and oil, adding it “made no sense” to invest in high carbon sources of energy. Kerry said the US would target “wasteful fossil fuel subsidies” at upcoming meetings of the G20 and Asia Pacific Economic Cooperation forum, which count the world's top coal users as members.

**Agribusiness**

- In a 40-page report, Oxfam America suggests several steps to improve Feed the Future, an Obama administration initiative that uses public-private partnerships to boost local food production in targeted countries. The program has made "substantial, real and important improvements" in U.S. food security efforts, but "the ambitious agenda embraced by U.S. AID remains a work in progress."

- The first case of H5N2 avian influenza in the U.S. South this year was confirmed on a turkey farm in northwestern Arkansas. A flock of 40,020 turkeys in Boone County, about 140 miles north-northwest of Little Rock, was hit. The USDA said the farm "is located within the Mississippi flyway where this strain of avian influenza has been previously identified."

- A rare coalition of grain processors, conservationists and clean-water groups asked the Agriculture Department to dedicate one-third of the Conservation Reserve to buffer strips, windbreaks and other practices that protect water quality and wildlife habitat.

- The Agriculture Department stopped all new research projects at its Meat Animal Research Center until new protocols are implemented in response to reports of the harsh treatment of animals at the facility in Nebraska, according to Feedstuffs. The USDA reviewed operations at the facility after a New York Times story described questionable practices.

- In Connecticut, legislation is being considered which would mandate GMO labeling on baby food and formula. The bill, HB 6798, has passed out of the Children's Committee by a wide margin of 10 votes in favor to 2 against. The bill would not fall under the trigger clause already in place in the state's GMO labeling law.

- Legislators and activists are working to gain approval for the GMO labeling bill A.617 in
New York which failed to pass last year. This year the bill has been approved by the Consumer Affairs Committee and supporters are focusing on rallying support in the Assembly.

- In Idaho, Resolution HJM 6 was passed in the state House of Representatives. The bill, proposed by Rep. Steve Miller urges US Congress to pass legislation forbidding GMO labeling on the state level and to outlaw mandatory GMO labeling.

Insurance/Healthcare

- Some Republicans in Congress have said that the billions of federal HITECH dollars spent to implement electronic health records have not yet resulted in systems interoperability that paves the way for secure national data interchange, which can improve treatment based on timely access to information. Now, Rep. Michael Burgess, M.D., R-Texas, is drafting legislation that calls for devising new methods for measuring whether EHR vendors are compliant with interoperability standards.

- A former customer service representative at Blue Cross Blue Shield of Michigan is among 11 individuals recently arrested in connection with an alleged identity theft scheme that affected more than 5,500 health plan members and resulted in hundreds of thousands of dollars in credit fraud.

- In several recent cases nationwide, nurses have used their access to patient and employee information to commit identity theft, demonstrating the challenge of protecting patient and employee information.

- To protect patient privacy, West Virginia United Health System is taking a multi-step approach to thwarting insider threats, including aggressive analysis of access audits. An auditing tool grabs reports from multiple clinical systems, including the organization's electronic health record system, and looks for signs of inappropriate access, such as staffers accessing records of patients with the same last name as theirs.

- While federal regulators flesh out details of a 10-year roadmap for electronic health record interoperability, which would pave the way for national data exchange, five GOP senators are demanding that more attention be paid to the plans for security and privacy of patient data as it's shared among healthcare providers.

Financial

Financial Services

Activism

- Activists conducted an 'Emergency People's Assembly to Fight Tax Foreclosures' in Detroit, MI on March 14. Participants planned actions to demand a moratorium on all tax foreclosures and evictions from occupied homes and to end water shut-offs.

- Occupy Wall Street will conduct a national strike against "slave/feudal" wages on April 14 in New York City with intent to "shut the city down."

- Restaurant labor activists conducted a minimum wage protest on March 13 in Chicago, IL, demanding a $15 minimum wage from the world’s largest fast food company.

- An Anti-TPP protest will occur on March 19 in Washington, DC in which participants will "flood" Congress.

- A protest against austerity policies employed by the Canadian Government will take
Activists will hold an anti-austerity protest at St. Paul's Cathedral in London, UK on March 18. The protest coincides with the release of the UK budget on that date.

Multiple activist groups conducted disruptive actions on March 14 in Greenwich, CT, targeting area hedge fund managers for their practice of "avoiding taxes, depleting schools, destroying jobs, and buying our politicians." The event included a protest action at an area hedge fund manager’s home residence.

An action against evictions conducted by a private-equity firm will take place in London, UK in the morning of Tuesday, March 17. Participants plan to picket the firm’s office as employees come into work.

Information Security Risk

Cybercriminals are still exploiting Brazil’s most popular payment method, Boleto Bancário, using sophisticated malware. The Boleto malware campaign previously had a reported potential loss of US$3.75 billion. Researchers found that criminals compromise victims' Firefox and Chrome browsers by installing malicious extensions to steal Boleto payment information. Bogus emails with fake threats of debt that must be paid to governments are used to get users to install these extensions.

A Troy, Michigan-based vendor of point-of-sale solutions for restaurants, corporate cafeterias, casinos, airports and other food service venues, was notified by law enforcement that some of its customer locations have been compromised in a potentially wide-ranging credit card breach.

Disguised as the Web version of a popular messenger app, a banking Trojan is being distributed via email. Cybercriminals send out email letters of invitation to download the desktop version of the mobile SNS platform especially popular among younger users. Messages contain a link supposedly leading to the official website of the app. However, upon clicking the link the user is taken to another, compromised, site where a malicious executable file is downloaded. Under the file hides a Trojan Downloader Win32/TrojanDownloader.VB.QRM. After the installation, the trojan loads on the infected computer another malware called Win32/Spy.Banker.ABOD, a spyware designed to steal authentication data for online banking. The mobile app’s number of users exceeded 700 million people by January of this year.

Hackers compromised the payment processing systems at a restaurant chain location in San Francisco, CA and may have accessed payment card information for a period of two months before the breach was contained. Between October 2 and December 4, 2014, malware lurked on the computer systems used for handling payment card transactions. The information that may have been exposed includes name, payment card account number, card expiration date, and security code.

Researchers are warning that the number of infections caused by the BandarChor ransomware with file encryption capabilities is on the rise. The malware usually arrives on the victim’s computer via a malicious email, but there is an indication that it may also be included in certain exploit kits.

A flaw in the Dropbox Android app could allow attackers to steal sensitive corporate data. Researchers claimed the flaw affects Dropbox SDK versions 1.5.4 to 1.6.1 and can be exploited locally using malware as well as remotely using drive-by techniques. It effectively allows an attacker to execute malware during a Dropbox log-in and obtain the “nonce,” a random number used to help authenticate the user. The hacker can then download to their own Dropbox account sensitive files from any vulnerable apps linked via SDK to the user’s compromised Dropbox account. There’s also the option of uploading files into the user’s compromised apps via Dropbox.

Both Apple and Microsoft released patches to fix the FREAK vulnerability that could help attackers intercept secured network communications. Discovered earlier this month, FREAK (Factoring attack on RSA-EXPORT Keys) provides a way for an attacker to intercept SSL-encrypted traffic encrypted by SSL (Secure Sockets Layer).
as it moves between clients and servers. An attacker could use the flaw to secretly access and even alter communications between two parties.

- A leading UK bank is developing a system where customers can log into their accounts on a smartphone by using their heartbeat as proof of identity. Instead of using a password or fingerprint, the app pairs over Bluetooth to a heart rate monitor worn on the customer’s wrist. Once the gadget has an example of the customer’s heartbeat rhythm recorded, it compares this to their current heartbeat each time they want to use the app.

**Legal, Litigation, Regulatory Risk**

- The U.S. Department of Justice charged three men in connection to the largest data breach ever, which exposed 1 billion e-mail records from more than 100 different businesses from 2009 to 2012. Two Vietnamese citizens, who were both residing in the Netherlands, have been charged with hacking into U.S. email service providers. A Montreal-based Canadian was also charged with helping the two men knowingly convert stolen email addresses into $2 million in profits via his affiliate marketing company.

- A class action lawsuit was filed against the largest U.S. bank by assets, alleging it engaged in racketeering and manipulation of California’s electricity market. The lawsuit, filed in California federal court on Monday, March 9th, accuses the firm of violating the Racketeer Influenced and Corrupt Organizations Act (RICO) when it sold power from several gas plants in the state between 2010 and 2012.

- A regional bank based in Irvine, California announced last week that it entered into a civil settlement with the United States Department of Justice, subject to court approval. The settlement concerned a single third-party payment processor, which the bank terminated in 2010 after it was recapitalized and a new management team was put in place. Under the settlement, the bank, without admitting liability, has agreed to pay $1.225 million to the United States and to abide by certain conditions if it decides to provide banking services to third-party payment processors.

- A new report by the Consumer Financial Protection Bureau said arbitration clauses in the fine print of credit card and checking account agreements harm consumers by limiting the compensation they can receive in disputes with financial firms. More than 75 percent of consumers didn’t know if they were subject to the clauses, many of which limit the ability to go to court to settle disputes. Fewer than 7 percent of those covered by arbitration provisions knew that the terms restricted the ability to sue or participate in class-action cases, the study found. Those class-action suits often produce larger payments to consumers than arbitration proceedings, the consumer bureau said. The provisions allow either the financial firm or the consumer to require that any dispute be settled by a private arbitrator instead of in court. The study’s findings are a prelude to the next step the bureau will take, which could be new regulations limiting the use of arbitration clauses.

- A leading, global fast food chain is suing the City of Seattle, WA for raising the city’s minimum wage to $15 per hour. The restaurant chain argues the new minimum wage violates the Constitution’s Equal Protection Clause, and that the clause should protect businesses rather than human workers.

**Operational Risk**

- A former employee at the largest American Internet-based retailer stole $18,260 from gift cards she issued, leaving customers with useless vouchers. The money was transferred to two separate bank accounts that were found to have almost no balances.

- An annual fraud report by a major credit reporting agency said that fraud-detection rates have increased during the past year, with around 50 fraud instances now being detected per 10,000 cases during Q4 2014, compared to 40 fraud instances detected per 10,000 cases in Q4 2013. The report also revealed a marked shift in the level of third-party or identity theft as a proportion of all detected fraud cases. The trend now
accounts for more than half (52 per cent) of all detected fraud cases. The report suggested that the switch reflects a return to pre-downturn levels of identity theft when it previously eclipsed first-party fraud (i.e. fraud carried out by a genuine person). Detected first-party fraud, as a proportion of all frauds, has now decreased from 60 per cent of all fraud cases in Q4 2013, to 48 per cent of fraud cases as at Q4 2014. But it continues to be most prevalent for mortgage products.

- An article reported that speakers at a financial conference in London, UK on Tuesday, March 10, warned bankers that they should watch what they say in public or risk a devastating computer network attack on their business from state-sponsored hackers. The article reminded that in January, two Russian citizens were charged by the FBI in the US for spying in New York. It is alleged that the two were working for the Russian SVR intelligence agency. Communications between the two centered on how exchange-traded funds might be used to undermine Wall Street, causing as much damage to the US financial system as possible.

**Reputational Risk**

- A new study by a coalition of Indonesian civil society organizations published its findings on the investment policies of the eight largest national banks and the three largest foreign banks operating in Indonesia in regards to their failure to address social and environmental elements in their core business policies. The report called for banks to immediately embark on improving their investment policies, placing social, environmental and human rights concerns at the heart of those policies. The report also advocated that banks must no longer ignore the issues of climate change, human rights, labor rights, tax evasion, and corruption.

- A new study by two Indonesian based firms identified multiple international banks lending to a group of 25 leading Indonesian palm oil businesses, all of which are controlled by wealthy tycoons, often via holding companies in tax havens. The Indonesian palm oil sector is believed to be contributing "serious environmental and social problems" via valuable forests being converted into plantations.

- An article reported that a GSE for housing is still engaging in behavior that could precipitate future financial crises and taxpayer losses according to a government report. The article said that the Federal Housing Finance Agency Inspector General stated his concerns involving the GSE’s “haphazard” decision to fill a critical auditor position with an employee who lacked proper qualifications and suffered from a conflict of interest. The Inspector General also pointed out that there is a “substantial risk” that the GSE will operate in an unsafe and unsound manner, suffer losses and expose U.S. taxpayers to further financial risks.

**Global Intelligence**

**Asia**

- An article on Sina.com.hk reports several official websites owned by Japanese companies and organizations were hacked and have been tampered with. According to the article, the attacks could have been launched by ISIS.

- An article on W010w.com.cn reports that Curtin University of Singapore suffered a hacker attack and its official website’s homepage was defaced. According to the article, ISIS was behind this attack.

**Brazil**

- On March 15 over a million Brazilians took to the streets to call for the impeachment of President Dilma over corruption in her party and across the government as the Petrobras corruption scandal continues. Unlike the nationwide protests that occurred in June of 2013 that cut across party lines and socio-economic strata to protest the sad state of public services and infrastructure, Sunday’s protest was a mass mobilization of
the half of the electorate that is embarrassed and deeply frustrated at Dilma and the
government. Unless Dilma gets directly implicated in the Petrobras scandal it is
unlikely that there is any viable basis for her impeachment. Calls by some of the
protesters for the military to take over the government will go unheeded by the most
professional Army in Latin America content to serve their constitutional role in support
of the nation’s civilian leaders.

Legal and Regulations

Some states have update their breach notification laws:

- **Montana** — Montana has amended its 10-year old breach notification law (see Mintz
  Matrix) to expand the definition of “personal information” and require notice to the state
  attorney general’s consumer protection office. H.B. 74

- **New Jersey** — Governor Christie recently signed legislation into law requiring health
  insurance companies in that state to encrypt personal information of policyholders.

- **Connecticut** — In the aftermath of the massive Anthem data breach, legislation has
  been introduced in the Connecticut General Assembly requiring a wide swath of
  insurance businesses to implement data security technology that encrypts personal
  information of insureds. See “Act Concerning the Security of Consumer Data”.

- **Washington** — The Washington House has unanimously passed a bill that would
  make the failure to notify consumers of a breach as required by the state’s data breach
  notification law a violation of the state’s Consumer Protection Act. (H.B. 1078) The
  measure would require notification to consumers — and the state’s AG — as quickly
  as possible and no later than 45 days after discovery of a breach of personal
  information such as a person’s name in combination with a Social Security number,
  driver’s license number or payment card number and payment card access code or
  password.

- **New Mexico** — New Mexico is one of three states without a data breach notification
  law. HB 217, the Data Breach Notification Act is working its way through state
  legislature.

- See the Mintz Matrix for more information on State Data Breach Notification Laws.

- Last week, the National Institute of Standards and Technology (NIST) released a
  preliminary discussion draft of its Framework for Cyber-Physical Systems. The goal of
  this draft: to create an integrated framework of standards that will form the blueprint for
  the creation of a massive interoperable network of cyber-physical systems (CPS), also
  known as the “Internet of Things.” In 2014, NIST established the cyber-physical
  systems public working group (CPS PWG)—an open public forum which includes
  representatives from government, industry, and academia—to develop the CPS
  framework. By creating a common framework at an early stage of the Internet of
  Things, the CPS PWG hopes to ensure the development of a secure, integrated, and
  interoperable ecosystem of connected devices. The CPS PWG will continue to solicit
  input as it refines the draft and works to finalize the framework for use in multiple
  industry sectors.

Pharmaceuticals
China had a backlog of more than 18,500 drugs awaiting approval by the end of 2014, up 33% from the previous year, according to the China FDA's Center for Drug Evaluation.

The Lebanese health minister filed lawsuits against Pfizer and Mectapharm, a distributor, for overcharging the state for medication used to treat Parkinson's disease.

In the latest dust up over prescription drug costs, Gilead Sciences and Vertex Pharmaceuticals shareholders will be allowed to vote on resolutions that would require the drug makers to publish reports evaluating the risks of the pricing policies for the medicines.

In a bid to resolve a long-running and controversial saga, the Johnson & Johnson unit that sells over-the-counter medicines has agreed to plead guilty to a misdemeanor and pay a criminal fine of $20 million for selling adulterated infant and children products. The McNeil subsidiary also agreed to forfeit $5 million, according to the U.S. Department of Justice. The move comes six years after McNeil first received complaints about unusual particles in bottles of Infants' Tylenol, but failed to conduct needed investigations to determine the cause or how to prevent a recurrence. By reaching the plea agreement, J&J hopes to put behind it an episode that eroded confidence among consumers, physicians and investors, although a key manufacturing plant remains offline.

Amen plans to cut about 300 jobs and close one of its South San Francisco buildings as part of a reorganization that will combine its cancer organization with Onyx Pharmaceuticals, which the biotech bought for $10.4 billion.

Retail

NEXTEP Systems, a Troy, Mich.-based vendor of point-of-sale solutions for restaurants, corporate cafeterias, casinos, airports and other food service venues, was recently notified by law enforcement that some of its customer locations have been compromised in a potentially wide-ranging credit card breach.

Aeropostale Inc. says it is considering closing as many as 75 additional stores despite reporting a smaller profit loss in the fourth quarter.

The Children’s Place Inc. on Thursday accelerated its store closing plans to 200 stores through 2017 (including 76 stores closed in 2013 and 2014), up from its previous announced target of 125 stores through 2016. The company also issued a weak outlook.

Revenue growth in Hong Kong this year will likely be the slowest in at least four years, hit by a drop in visitors from the mainland who have been put off in part by rising hostility among Hong Kongers.

Technology

Security firm enSilo, based in Israel, today officially launched and introduced a real-time endpoint security tool for preventing the exfiltration of data by attackers. The tool looks for malicious connection attempts from the machine to the outside, and shuts them down so intruders can't take anything with them on the way out.

CloudFlare, one of the larger DNS providers and a performance and security specialist, is introducing a new service called Virtual DNS that is designed to help protect against these new attacks and speed up organizations’ infrastructures. The service works by having organizations point their name servers to CloudFlare’s
Smartphone camera apps could soon do more than just capture images. Software integrated with a new line of smartphone chips will be capable of recognizing, say, a cat or city skyline in a photo, and tagging pictures of your friends with their names. The technology, which Qualcomm calls Zeroth, could make sophisticated machine learning more common on mobile devices.

U.S. technology companies need to confront difficult choices amid new bank-security rules in China, as Beijing offers few signs that it will abandon measures that could limit the IT firms’ sales to the big market. Banks faced a Sunday deadline to submit plans to Chinese officials on how they will convert their internal technology into what Beijing considers secure and controllable systems.

A British parliamentary committee has recommended that information such as web browsing history and location tracking data be given an extra level of protection against government spying.

Cisco Systems’ Talos researchers reported to Google that private information such as names, physical and email addresses, and phone numbers belonging to 282,867 domains registered through Google Apps’ registrar, eNom, were leaked for nearly two years due to a software defect that did not extend the company’s unlisted registration service, potentially exposing them to spam, spear-phishing attacks, or identity theft.

Telecommunications

- Facing mounting costs for pay-TV, a new TiVo study revealed that 1.5 million U.S. consumers are planning to break ties with their satellite or cable pay-TV provider by subscribing to an over the top (OTT) video service.

- The FCC has delivered its long-awaited net neutrality order that reclassifies ISPs under Title II of the Communications Act, one that will open a host of legal challenges from major telcos like AT&T and Verizon.

- A Dutch court Wednesday handed a victory to privacy advocates by striking down a data-retention law that gives the government easy access to telecommunication data. The District court of The Hague said the law, which requires telecom providers to collect and store data for as long as 12 months, violates citizens’ right to privacy and the right to protection of personal data. “The judge finds that this violation is not limited to what is strictly necessary,” it said.

Defense

- From the Snowden revelations we learned not only about NSA data collection projects, but also about many software tools that are used to analyze and search those data. These programs run on secure computer networks, isolated from the public internet. Here we will provide an overview of these networks that are used by the US military and US intelligence agencies. Besides computer networks, they also use a number of dedicated telephone networks, but gradually these are transferred from traditional circuit-switched networks to Voice over IP (VoIP). This makes it possible to have only one IP packet-switched network for both computer and phone services. It seems that for example NSA’s NSTS phone system is now fully IP-based.

- An individual suspected to have stolen data from the global communication system used by the US Department of Defense (DoD) has been arrested by the officers of the National Crime Agency in UK. The hacker, 23, allegedly breached the computer
network of DoD on June 15, 2014, and exfiltrated information from the Enhanced Mobile Satellite Services, a communication system used for contacting DoD employees around the world via email or phone. Although the incident did not result in loss of sensitive information, it seems that the hacker managed to obtain contact details (names, titles, email addresses and phone numbers) of 800 individuals as well as the IMEI (International Mobile Station Equipment Identity) codes for about 34,400 devices; the code identifies both mobile and satellite phones.

- CIA director John Brennan publicly issued a memo to the agency’s staff calling for a massive re-organization of its hierarchy and priorities. And center stage in the CIA’s new plans is a new Cyber Directorate that will treat “cyber”—in federal-speak, hackers and hacking—as a major new focus for both offense and defense. The CIA’s announcement represents yet another sign that cyber-offense is gaining importance for practically every intelligence and military agency. The FBI late last year asked for new rules of criminal procedure that would vastly expand its power to hack into the computers of criminal suspects.

- The Wikimedia Foundation on Tuesday joined with other rights groups to file suit against the US National Security Agency's spying program— in particular, its large-scale search and seizure of internet communications, commonly referred to as upstream surveillance.

- China’s President Xi Jinping has outlined a requirement for China to strengthen civil-military integration (CMI), the process through which Beijing aims to enhance military capabilities by leveraging innovation from the commercial sector. Speaking to a People’s Liberation Army (PLA) delegation on 12 March, President Xi said CMI processes were in need of reform in order to “break new ground” in developing the PLA’s capabilities.

---

**Law Enforcement**

- A 20-year-old man charged Sunday with shooting two police officers who were keeping watch over a demonstration outside the Ferguson Police Department had participated in the protests earlier that night, police said. St. Louis County Prosecutor Robert McCulloch said Jeffrey Williams told authorities he was firing at someone with whom he was in a dispute, not at the police officers. Williams is charged with two counts of first-degree assault, one count of firing a weapon from a vehicle and three counts of armed criminal action. McCulloch said the investigation is ongoing.

- The FBI is investigating the apparent firebombing of a KFC in Reno after authorities found the initials of an animal rights group scrawled on a drive-thru sign, The Associated Press reports. Investigators believe a window was broken at the restaurant, and flammable liquid was found inside, in what may be a domestic act of terrorism. The initials – ALF – stand for Animal Liberation Front, a group of environmental advocates who have firebombed laboratories and other places linked to animal cruelty. Another KFC was firebombed in February 2014 in New Zealand, and ALF took credit.

- Authorities in Wisconsin say a likely cyberattack has affected the city of Madison’s website and email system, as well as computers used by law enforcement countywide. Dane County Emergency Management said the city began experiencing a high volume of Internet activity consistent with an outside attack late Monday. The apparent attack comes three days after a Madison police officer on Friday shot and killed an unarmed 19-year-old. Similar attacks have occurred in other communities after officer-involved shootings, including in Ferguson, Missouri, after the death of Michael Brown.

- The Wall Street Journal reports the Justice Department’s newest electronic dragnet—plane-mounted “dirtboxes” that can slurp thousands of cellular phone ID’s from the air which was originally developed by the CIA to hunt terrorists in the Middle East is now being used domestically to track American citizens. These dirtboxes are electronic
sniffers that mimic cellular tower signals to incite any cellular telephone within range to broadcast its identifying registration information to law enforcement.

- Michigan State Police have become one of the first law enforcement agencies in the nation to receive authorization from the Federal Aviation Authority to use unmanned aerial systems, commonly referred to as drones, in police operations.