Welcome to the Cyveillance Weekly Trends Report

Greetings from Cyveillance, the leader in open source threat intelligence. Since threat intelligence is constantly evolving, we publish this newsletter to keep our customers updated on the latest threats to various industries. Each week, we’ll send you highlights from our analyst research reports. You can unsubscribe at any time. For the latest security news stories throughout the day, you can also follow us on Twitter, or to view the latest security articles from Cyveillance experts, subscribe to our blog.

In this Issue:

- Top Weekly Incidents
- Energy
- Agribusiness
- Insurance / Healthcare
- Financial Services
- Global Intelligence
- Legal and Regulations
- Pharmaceuticals
- Retail
- Technology
- Telecommunications
- Defense
- Law Enforcement

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

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

Top Incidents

Energy

- The group, Beyond Extreme Energy has announced a mass call of action to “Return to FERC” on May 21-29 in Washington DC. The group opposes FERC rubber-stamping fracked gas projects and wants to “stop FERC and put a pinch on corporate profits from exploitation and the permitting process altogether!”

Agribusiness

- Dairy companies have been fined €88m for fixing milk prices paid to Spanish farmers over thirteen years. Eleven businesses, including the Spanish wings of dairy giants Danone, Nestlé and Lactalis, have been punished for anticompetitive practices by the country’s competition watchdog.
Insurance/Healthcare

- The recent cyber-attack against Anthem Inc. that exposed personal information on 78.8 million individuals is just the latest siren that the healthcare threat landscape is becoming more menacing. But while cyberthreats are rising, budgets for information security are not at many healthcare organizations.

Financial Services

- Security experts discovered a potentially catastrophic flaw known as FREAK (Factoring attack on RSA-EXPORT Keys) that for more than a decade has made it possible for attackers to decrypt HTTPS-protected traffic passing between Android or Apple devices and hundreds of thousands or millions of websites, including high-profile government, Fiserv, and media sites. A recent scan of more than 14 million websites that support the secure sockets layer or transport layer security protocols found that more than 36% of them were vulnerable to the decryption attacks. Microsoft recently announced the security vulnerability affects all Windows users.

Global Intelligence

- Four of the five ex-ministers in President Dilma’s cabinet received at least four million Reals from the Petrobras corruption scheme along with monthly stipends of R$ 30,000 to R$150,000. They have now been charged in the ongoing investigation.

Legal and Regulations

- The U.S. charged three foreigners for allegedly stealing one billion email addresses in what the Justice Department described as "one of the largest" instances of data fraud ever, Reuters reports. Though the government declined to say which companies were attacked, security blogger Brian Krebs reported that one of the victims was the email marketing firm Epsilon, a unit of Alliance Data Systems Corp.

Pharmaceuticals

- Health Canada is ramping up inspections of pharmaceutical manufacturing plants and will be publishing its findings online, and the regulator also told companies that it intends to increase “the frequency of planned and unplanned” inspections of facilities, according to The Star. The Star investigation revealed that FDA inspectors have found extensive problems at Canadian drug companies.

Retail

- Mandarin Oriental Hotel Group confirmed on March 4 that the company is investigating a potential malware infection that breached the point-of-sale (PoS) systems in some of the chain’s 24 locations worldwide, including hotels in the U.S., which impacted an unknown number of customers. The investigation was initiated after financial institutions reported a pattern of fraudulent charges on payment cards used at Mandarin hotels dating back to December 2014.

Technology

- ASML, a Netherlands-based machine manufacturing company for integrated circuits have been breached. The company stats that it hasn’t determined the identity of the attackers, but anonymous sources have cited that the attack was carried out by Chinese government.

Telecommunications

- A group of hackers calling themselves Team Hans managed to gain access to corporate information belonging to Canadian telecommunication and media company Rogers Communications relying mostly on their charm. The dump is over 400MB in size and contains contracts with corporate customers, business emails, sensitive employee information (ID, documents), as well as credentials for the VPN (virtual private network), which would allow access to the internal computer infrastructure of
Defense

- Significant security weaknesses in the Federal Aviation Administration’s information security program have placed the nation’s air traffic control system at risk of being hacked, according to a Government Accountability Office audit report released Monday.

Law Enforcement

- The FBI is investigating the hacking of several business websites in the U.S. that showed a black ISIS flag on the homepage. NBC News reports that the home pages showed the words, “hacked by ISIS, we are everywhere,” with a link to a Facebook page that doesn’t exist. What appeared to be an Arabic song played in the background. The targets included Eldora Speedway in Rossburg, Ohio, owned by NAS

Energy

- Senator Sheldon Whitehouse (D-RI) was interrupted during his keynote address at Yale University’s “New Directions in Environmental Law” conference by members of the Connecticut-based climate justice collective Capitalism vs. the Climate with a “laugh riot”. Each time the Senator suggested he was a climate champion, the demonstrators roared with hearty laughter. The demonstrators stated, “It’s a joke that Senator Whitehouse is an environmentalist. He needs to stop supporting Spectra’s fracked gas pipeline expansion. He’s not a climate champion. He’s a climate clown.” They then walked to the stage and held a banner reading “Fracked Gas Kills” in front of the Senator. Prior to the speech approximately thirty demonstrators protested outside the conference in opposition to fracking.

- Member of FANG: Fighting Against Natural Gas completed a 28 mile march from Burrillville to Providence RI to converge at the State House to visit Governor Raimondo, who wouldn’t meet with them. They continued on to the Department of Health, the Department of Environmental Management and then dropped a banner at Providence Place Mall. The group ended their day at Senator Sheldon Whitehouse’s office where they sang and “set our intention to continue to lay down or bodies and souls until we #StopSpectra.”

- The group, Beyond Extreme Energy has announced a mass call of action to “Return to FERC” on May 21-29 in Washington DC. The group opposes FERC rubber-stamping fracked gas projects and wants to “stop FERC and put a pinch on corporate profits from exploitation and the permitting process altogether!”

- The Senate failed on Wednesday to override President Obama’s veto of legislation approving the Keystone XL oil sands pipeline, falling five votes short of the two-thirds majority needed in a 62-37 vote. It’s the first time Congress has voted on whether to override a veto from Obama and could be a sign of things to come, with Republicans in charge of the House and Senate.

- Power Engineering reports that Saudi Arabia and South Korea have signed a deal to build nuclear power plants in the Kingdom. The two governments signed a memorandum of understanding to conduct a three-year preliminary study on the feasibility of building the reactors in Saudi Arabia, according to utilities-me.com. South Korean companies would build two small- to medium-sized reactors for around $2 billion. The deal builds upon a similar agreement signed in 2011. Korea Electric Power Corp. is currently building a four-unit, 1,400-MW nuclear plant in Abu Dhabi in the UAE. The first of the units is expected to come online in 2017, with all four operational by 2020. Saudi Arabia had planned to add 17 GW of nuclear power capacity by and 41 GW of solar by 2032 but recently pushed the deadline back to 2040.

- Legal experts from across Canada are urging all parliamentarians to “ensure that C-51
not be enacted in anything resembling its present form.” They argue, in an open letter published on the National Post, that the federal government’s anti-terrorism bill is a “dangerous piece of legislation” that has not been given due debate. The Harper government decided to cut off a second reading debate of the bill on February 23, after less than three days of discussion. The authors of the letter note the lack of debate is a “troubling undermining of our parliamentary democracy’s ability to hold majority governments accountable.”

- Activists in Albany, NY are planning a climate justice rally to influence Statehouse politics on April 22.
- Youngstown State University, in Youngstown, OH, is hosting three anti-fracking events on March 13 & 25, and on April 6.
- Libya’s civil war has accelerated its disruption of the nation’s oil industry, with the state oil company declaring force majeure on 11 oilfields due to combat proximity.
- The Christie Administration in New Jersey has reached a settlement with ExxonMobil over longstanding environmental allegations. The settlement is a small fraction of the damages originally sought, leading to animated complaints by environmentalists throughout the state.
- Activists in the Portland, OR area have multiple upcoming anti-oil train events. This may indicate that oil train disruption will once more be a theme in Pacific Northwest activism this coming spring and summer.
- Greenpeace is planning a March to Stop Deep Sea Oil in Auckland, NZ on March 29. The event is planned to finish at the location of a major international oil conference. This is expected to be a large gathering, with multiple environmental groups attending and promoting the event.

### Agribusiness

- Attacks the past two weeks on at least 16 farms across several rural South Carolina counties killed an estimated 300,000 chickens and cost the owners roughly $1.7 million. Clarendon County Sheriff Randy Garrett said someone familiar with alarm systems used in chicken houses is responsible. Those alarms also control the heat, air conditioning and ventilation units and notify farmers by cellphone when buildings get too hot or cold. Chickens can die in about an hour if the ventilation and heating systems are turned off.
- Ukraine’s recession is threatening to cause the worst decline in the corn harvest since 2005 as soaring interest rates make borrowing too costly.
- The National Bio- and Agro-Defense Facility, for research into some of the most feared livestock diseases, was allotted $300 million as part of congressional approval of funding for the Department of Homeland Security. The laboratory will replace the USDA’s Plum Island Animal Disease Center, which has been in operation since 1954.
- A WTO panel expects to rule by mid-May on whether the United States violates global trade rules with its requirement for packages of beef, pork and poultry to say where the animals were born, raised and slaughtered.
- Japan and the United States resumed talks on the 12-nation Trans Pacific Partnership trade pact, “but the outcome of the negotiations remains unclear with political difficulties mounting for Prime Minister Shinzo Abe and indications of growing opposition in the United States.”
- While the proposed Trans Pacific Partnership and U.S.-EU trade pacts get the headlines, the African Growth and Opportunity Act also is due for action this year. In a report, the Chicago Council on Global Affairs suggests creation of a U.S.-Africa Food
Dialogue to improve food security in the continent and position U.S. businesses to participate in a food and agriculture market expected to be worth $1 trillion by 2030.

- Canada’s latest case of mad cow disease, reported on Feb. 13, was born on the same farm in Alberta as an animal afflicted with the brain-wasting disease in 2010.

- Dairy companies have been fined €88m for fixing milk prices paid to Spanish farmers over thirteen years. Eleven businesses, including the Spanish wings of dairy giants Danone, Nestlé and Lactalis, have been punished for anticompetitive practices by the country’s competition watchdog.

- McDonald’s plans to stop buying chickens that have been reared on antibiotics meant for humans within two years in response to growing concerns about resistance to antibiotics.

- The second Public Board member was officially announced by Factor GMO on March 2, 2015. Actor and UNICEF Goodwill Ambassador for the Middle East and North Africa, Mahmoud Kabil, was announced as the latest to join the Public Board for the largest and most comprehensive GMO safety study, set to begin later in 2015.

- On March 2, 2015, AllAfrica reported on the announcement by Gambian president Yahya Jammeh that Gambia will never accept GM food. The announcement came as part of his speech opening the 2015 legislative year at the State Opening of the National Assembly in Banjul, Gambia. Jammeh asserted that the country is dedicated to using organic farming techniques for all produce used both for domestic consumption and for export.

- In Accra, Ghana, the Fast Track High Court sat to hear more arguments related to the lawsuit being brought by Food Sovereignty Ghana (FSG) against the Ministry of Food & Agriculture and the National Biosafety Committee. The National Biosafety Authority and the Attorney General’s department have been added as the 3rd and 4th defendants in the case. There has been a halt to commercialization and development of GM crops in Ghana until the case concludes. The hearings have been postponed until April 2, 2015.

- On March 4, 2015, the book "Altered Genes, Twisted Truth" will be released in London written by public interest attorney Steven Druker. The book describes how the US government and leading scientific institutions have misrepresented facts about GMO's which call into question the safety of such products. The book has a forward by Jane Goodall who asserts the great importance of this book.

- On March 3, 2015, Rainforest Action Network published this article promoting the publication of their report on human rights abuses, including child labor violations, associated with palm oil production. The report is titled "Free and Fair Labor in Palm Oil Production: Principles and Implementation Guidance." RAN collaborated with labor advocacy groups from Indonesia and Malaysia as well as with international NGO's in the production of this report.

- New York state legislatures are currently pursuing mandatory GMO labeling legislation. Assembly member Linda Rosenthal has sponsored the bill A00617 and State Senator Ken LaValle has sponsored the bill S00485. On social media, activist groups are calling on followers to contact their legislators to request support for these bills.

- In Brazil, direct action was taken by activists in several instances this week opposing GE trees. Farmers disrupted a meeting of the Brazil National Biosafety Technical Commission (CTNBio) deciding to release three varieties of GE plants in Brazil, and a decision by the commission was postponed. Activists also occupied operations of FuturaGene at many locations around Brazil destroying GE eucalyptus saplings being raised.
Since the Personal Health Information Protection Act (PHIPA) came into force in 2004 in Ontario, it has resulted in zero completed prosecutions — despite more incidents and high-profile breaches. The lack of action has been attributed to the authorities who preside over the act being unsure of the protocols for launching prosecutions and the government not believing a recommendation from the privacy commissioner to lay charges is enough to act upon.

A nurse with a history of narcotics theft illegally accessed a state database that contains prescription drug records for 1 million Minnesotans, all under the supervision of government entities that cost taxpayers hundreds of millions of dollars annually. Despite the nurse's background, he was given access to the database by both the Minnesota Department of Human Services and the state's largest insurer, Blue Cross and Blue Shield. The state database contains the names, addresses, and prescription records for 1 million Minnesotans and was set up in 2010 to monitor the abuse of prescription drugs.

Offering two years of free credit monitoring/credit restoration services to breach victims used to be considered unusual and commendable. But consumers have often noted that a breach of their SSN and identity information creates a life-long risk, with criminals able to sit on the data until after the free credit monitoring expires and then begin using it with less risk. Could the Anthem breach may become a game-changer on remediation offered to breach victims?

The recent cyber-attack against Anthem Inc. that exposed personal information on 78.8 million individuals is just the latest siren that the healthcare threat landscape is becoming more menacing. But while cyberthreats are rising, budgets for information security are not at many healthcare organizations.

Identity fraud reported by U.S. consumers dropped 3 percent in 2014, according to Javelin Strategy & Research's just-released report, 2015 Identity Fraud: Protecting Vulnerable Populations. While ID fraud usually refers to fraud perpetrated for financial gain, such as the takeover of a bank account or compromise of a credit card, it also can include medical fraud and new-account fraud, among other types of fraud.

Financial

Financial Services

Activism

A blog post urged supporters to contact a leading U.S. bank headquartered in San Francisco, CA and demand a foreclosed property in the city be returned to its previous owner.

Multiple Occupy Wall Street offshoot groups participated in an International Women's Day march on March 8 in New York City.

An anarchist-affiliated 'March Against Capitalism' action occurred on March 7 in Seattle, WA.

An online petition by the largest federation of unions in the United States criticizing big banks for providing compensation packages to executives who leave for high-level government positions indicated the group will deliver the petition to the CEOs of several major U.S. banks.

Activists conducted demonstrations outside several Federal Reserve banks on March 5 to highlight elevated unemployment among minority communities and urged officials not to raise interest rates any time soon. Protests occurred outside the regional Federal Banks of New York (NY), San Francisco (CA), Kansas City (MO), Philadelphia (PA), Minneapolis (MN), St. Louis (MO), Charlotte (NC), and Dallas (TX).
Disobedient mass action, demonstrations, blockades and other forms of direct actions around the new headquarters for the European Central Bank in Frankfurt, Germany will take place on March 18. Participants intend to sabotage the grand opening gala where several European state leaders and the European finance representatives will be present.

Occupied Wall Street and allied groups held their recurring 'Moral Mondays' meeting on March 9 on Wall Street in NYC to discuss "the immorality of Broken Windows policing and what can be done about it."

Housing activists will hold a 'Emergency People's Assembly to Fight Tax Foreclosures' in Detroit, MI on March 14 to plan future direct actions at the assembly.

Housing activists held a support rally for a homeowner in Dearborn, MI on March 7 to demand that a property investment firm that purchased the property at a foreclosure auction sell back the home to the previous owner.

An 'Occupy Rupert Murdoch' week of action against the media billionaire will occur March 23 through 29 outside Rupert Murdoch's new headquarters in London, UK. Participants will protest "against the billionaire-owned corporate media and its corruption of our democracy."

Labor activists will conduct rallies across the U.S. from March 9th through April 15th demanding that the minimum wage be increased to $15 per hour.

Workers at a Portland, OR state university conducted a rally on March 6th in Portland to demand fair contract rights and a $15 minimum wage.

Information Security Risk

Investigators traced a pattern of fraud on customer credit and debit cards suggesting that hackers tapped into cash registers at a national grocery chain's locations across the country. The grocery chain said it is investigating "a potential data security incident involving an unauthorized intrusion targeting limited customer payment card data."

A North Carolina-based credit union began notifying an undisclosed number of individuals that one of its laptops containing personal information, including Social Security numbers, cannot be located. The issue was discovered on January 31 and the laptop included password protected authentication.

Fraudsters are taking advantage of new exploits linked to a popular mobile payment method launched last year by the largest American handset maker. The problem is linked not to a compromise of the mobile device's security, but to lax authentication practices used by the banking institutions to verify cards that are loaded to the mobile phone for making purchases. One industry expert said issuers have been talking about fraud levels as high as 6 percent - the equivalent of millions of dollars in fraudulent transactions.

Security experts discovered a potentially catastrophic flaw known as FREAK (Factoring attack on RSA-EXPORT Keys) that for more than a decade has made it possible for attackers to decrypt HTTPS-protected traffic passing between Android or Apple devices and hundreds of thousands or millions of websites, including high-profile government, Fiserv, and media sites. A recent scan of more than 14 million websites that support the secure sockets layer or transport layer security protocols found that more than 36% of them were vulnerable to the decryption attacks. Microsoft recently announced the security vulnerability affects all Windows users.

A new financial malware dubbed 'Tsukuba' exclusively targets Japanese financial institutions. The Trojan is capable of harvesting victims' online banking credentials, personally identifiable information (PII) and even clear images of official identification documents. What makes Tsukuba potent is the fact that banking customers in Japan are less accustomed to seeing Trojan attacks in their region than those in English-speaking countries. The language barrier, one factor authentication that has protected some companies from fraud, also serves to keep their general population more naïve.
to the threat and, therefore, less suspecting of Tsukuba’s unique methods. Tsukuba is a banking Trojan from the proxy changers family. Its main goal is to manipulate the browser on infected endpoints to redirect victims to malicious URLs set up by the botmaster, then interact with these victims in order to extract credentials and PII from them.

- A new malware dubbed ‘PwnPOS’ is infecting point-of-sale (POS) systems. The malware may have been active since 2013. Made of two components, a RAM scraper binary and a binary responsible for data exfiltration, PwnPOS works similarly to most other known POS malware. It enumerates all running processes, searches for payment card data, and dumps it into a separate file. PwnPOS then compresses, encrypts, and exfiltrates it via an email to a pre-defined mail account via SMTP with SSL and authentication. The malware ensures its persistence and hides on the machine by adding and removing itself from the list of services to download and deleting files as needed to masquerade malicious files as benign ones. It also hides them within the %SYSTEM% directory, to store the stolen data in a .dat file that doesn’t appear out of place in the %SystemRoot%\system32 directory.

- An international upscale hotel chain headquartered in Hong Kong confirmed that its hotels were affected by a credit card breach. The hotel declined to comment on how many of the company’s two-dozen or so locations worldwide may be impacted. Banking industry sources said the breach almost certainly impacted most if not all of its hotels in the United States, including locations in Boston, Florida, Las Vegas, Miami, New York, and Washington, D.C. Sources also said the compromise likely dates back to just before Christmas 2014.

**Legal, Litigation, Regulatory Risk**

- An assemblyman in the California Assembly proposed AB 1326, a bill that provides guidelines for any individual or business that wants to start using virtual currency. AB 1326 says that any applicant who wants to pursue using virtual currency needs to pay $5,000 to the Commission of Business Oversight commissioner and provide basic information about their business and plans for virtual currency. Furthermore, the bill would require each licensee to maintain enough capital in case the commissioner discovers a problem with their business operations. To satisfy this capital requirement, applicants need to invest an aggregate amount equal to the value of the virtual currency that the licensee has on deposit for its customers in specified investments.

- The European Banking Authority (EBA) launched a three-month public consultation on its Guidelines on sound remuneration policies last week. These draft Guidelines set out the governance process for implementing sound remuneration policies across the EU, as well as the specific criteria for mapping all remuneration components into either fixed or variable pay. Guidance is also provided on the application of deferral arrangements and the pay-out instruments ensuring that variable remuneration is aligned with an institution’s long-term risks and that any ex-post risk adjustments can be applied as appropriate.

- An article reported that faced with increased regulation beginning in 2017, major U.S. banks are taking a number of restructuring steps, shedding staff and some speculative businesses, and cutting bonuses. Taking a “machete to expenses,” the article said, banks are speeding up disinvestments, trimming administrative budgets and turning to automation to replace employees in a broad array of banking operations, including online. The largest U.S. bank in terms of assets, for example, plans to save nearly $5 billion by 2017 and is closing 300 bank branches.

- A county hospital in Washington State is suing a leading U.S. bank to recoup some of the losses from a $1.03 million cyberheist that the healthcare organization suffered in 2013. The county alleged breach of contract, noting that the agreement between the county and the bank incorporates rules of the National Automated Clearinghouse Association (NACHA), and that those rules require financial institutions to implement a risk management program for all ACH activities; to assess the nature of the County’s ACH activity; to implement an exposure limit for the County; to monitor the County’s ACH activity across multiple settlement dates; and to enforce that exposure limit. The
lawsuit alleges that the bank failed on all of those counts, and that it ran afoul of a Washington state law governing authorized and verified payment orders.

**Operational Risk**

- A New York-based bank began notifying an undisclosed number of customers that their personal information was on a laptop that was stolen from an employee. A letter sent to customers stated the theft occurred on January 26th. There is no indication the personal information was used maliciously.

- New credit card technology which comes with embedded computer chips is believed to address only a narrow range of security issues. An open source article said that although chip-embedded cards are far more difficult to clone than the conventional cards, counterfeit cards account for only about 37% of credit card fraud, and the new technology will be nearly as vulnerable to other kinds of hacking and cyber-attacks as current swipe-card systems.

**Reputational Risk**

- According to a new whitepaper, the Federal Reserve’s 12 regional banks are “unconstitutional” and contribute to the popular misperception that the central bank is a privately owned institution not fully accountable to the public interest. The central bank is a public institution created by Congress. Both its chair and other members of its powerful seven-seat board of governors are appointed by the U.S. president and subject to Senate confirmation. However, the presidents of its regional reserve banks are appointed by a board of directors comprising mostly of private-sector representatives heavily influenced by the banking sector, though the appointments are subject to approval by the board. The paper asserted that this system violates constitutional law because the regional Fed bank presidents are public policy makers who are picked by a quasi-private structure, and that the president has no authority to remove them without going through three distinct steps.

- A Co-Chief Executive Officer of a leading German bank and four former managers were ordered to stand trial on fraud charges related to the bank’s handling of a dispute over the collapse of a late German business tycoon’s media empire. The trial is scheduled to begin in Munich starting April 28. The men were charged last year with aggravated attempted fraud for allegedly lying in response to a lawsuit filed by the famed, one-time media magnate. The bank must participate as an associated party in the case. The charges are part of the legacy of the 12-year-long dispute that the bank sought to end when it settled with the media group’s heirs last year.

- The UK government’s Serious Fraud Office launched an investigation into the Bank of England’s money-market auctions amid fears that they may have been hit by the rigging scandal that has engulfed the City. The SFO revealed on Wednesday (March 4) that it is investigating material referred to it by the Bank of England concerning liquidity auctions during the financial crisis in 2007 and 2008.

---

**Global Intelligence**

**Brazil**

- Data from the Ministry of Development, Industry and Foreign Trade (MDIC) on 2 March 2015, showed the value of imports exceeded those of exports by US$2.842 billion in February 2015, marking the highest recorded deficit for that month since 1980. The trade imbalance was also more severe than market projections, which had forecast on average a US$2.4 billion deficit. Total exports for 2015 through the end of February total US$25.796 billion, exceeded by a total of US$31.812 billion in imports.

- Consumer prices in Brazil rose more than expected in February, putting the 12-month rate at the highest level in nearly 10 years and underlining one of the main challenges
facing Brazil. The rolling 12-month IPCA increased 7.70% through February, well above the 6.5% ceiling of the central bank's target range. The 12-month figure marked the highest level since May 2005.

- There are six soccer players in the Richest Top 20 who are under 30, but only one under 26. That man is Neymar, 23, who comes in third with an estimated net worth of 135 million euros ($149 million). Timing was everything for Neymar. Every company wanted to be part of the World Cup, and Brazil's star player was an advertisers' dream. Even if the economy was not as strong as it had been, Brazil is a country of over 200 million people and they all need toothpaste, a bank, deodorant or car batteries (he was the face of all those products).

- Four of the five ex-ministers in President Dilma's cabinet received at least four million Reals from the Petrobras corruption scheme along with monthly stipends of R$ 30,000 to R$150,000. They have now been charged in the ongoing investigation.

China

- An article on Ce.cn reports that Tencent detected a malicious trojan that targets Windows, Android and iOS, in order to steal account passwords and personal information. The malicious trojan uses pornographic images and suggestive text luring users to click on a link which redirects users to a pornographic website.

- D1net.com reported a security vulnerability on the Google map plugin, where the Joomla server of the plugin could be exploited by the attackers and used as a tool for launching DDoS attacks.

- An article on Heilongjiang.dbw.cn reports that 40 websites in Heilongjiang, China were hacked and tampered with. In additional, 38 websites were being injected with backdoor vulnerabilities.

North America

- Broadband reported that Verizon, AT&T, and T-Mobile have acknowledged their mobile payment service SoftCard has failed and that they are selling the project to Google. Users are now being emailed and told that as of 3/31/2015 SoftCard will stop working entirely, and that those users should immediately proceed to download Google Wallet.

- BroadBand reported that top cable companies managed to net 80% of the total broadband additions in 2014, and continue to dominate the U.S. broadband landscape. According to the data from Leichtman Research Group cable operators saw a net gain of 2.65 million broadband subscribers last year - a 123% jump from the adds seen the year before. AT&T and Verizon continue to back away from DSL markets they don't want to upgrade, and as a result the top phone companies added just 345,000 net subscribers last year. That's 72% of the total net additions for the top telephone companies in 2013.

- According to a study by JD Power and Associates, Verizon Wireless once again ranked number 1 in all geographic regions. The study ranks carriers based on ten criteria: dropped calls; calls not connected; audio issues; failed/late voicemails; lost calls; text transmission failures; late text message notifications; Web connection errors; slow downloads; and email connection errors.

- Re/Code reported that Sling TV, Dish Network's Web-TV service, has been open to U.S. customers for just over a month and has at least 100,000 people signed up to check out the $20-a-month service. Dish and Sling say they're targeting an audience of around 10 million millennials who have broadband access but don't have traditional TV subscriptions, though Sling's marketing suggests it's going after cable-TV customers.

- Electronista reported that Tennessee Representative Marsha Blackburn has pushed forth two bills that attack the FCC's recent decisions on municipal broadband and net neutrality. In the case of the former, the FCC voted to pre-empt protectionist state laws that prevented towns and cities from improving or expanding their own broadband.
infrastructure. Meanwhile, Blackburn has also introduced her "Internet Freedom Act" which aims to overturn the FCC's new Title II based network neutrality rules.

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

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

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

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

---

**Legal and Regulations**

- In November 2014, the National Association of Insurance Commissioners – to get a better handle on cybersecurity risks. the NAIC formed the Cybersecurity (EX) Task Force to monitor emerging cyber risks and their impact on the insurance industry, determine whether any regulatory action may be required, and generally coordinate issues related to insurance and cybersecurity. This is the NAIC’s key initiative for 2015, and one of their expressed goals is to propose additional guidance to insurance examiners reviewing insurance companies’ practices for cybersecurity risks. To that end, the NAIC is considering collecting information from insurers writing cybersecurity coverage to learn more about this new and quickly evolving market.

- The Better Business Bureau has updated the BBB Code of Advertising for the first time since the 1970s “to reflect the many new ways advertisers reach consumers via websites, social media, texting and other channels.” While the truth-in-advertising principles remain the same, the Code now deals with 21st-century ad mediums like social media (i.e., Facebook and Twitter) and texting. Importantly, the Code was updated to include language for testimonials and endorsements that aligns the organization with the Federal Trade Commission’s stance as found in the agency’s Guides on Testimonials and Endorsements. To read the updated BBB Code of Advertising, click here.

- The Hill reports that the GOP is bracing for an Obamacare win in King v. Burwell, which will decide the fate of insurance subsidies for millions of low-income Americans.

- The CIA is doubling down on digital, with Director John Brennan announcing changes that include a renewed focus on cybersecurity and an office that will focus on integrating digital tools into the agency's work. The Hill has the story.

- The U.S. charged three foreigners for allegedly stealing one billion email addresses in what the Justice Department described as “one of the largest” instances of data fraud ever, Reuters reports. Though the government declined to say which companies were attacked, security blogger Brian Krebs reported that one of the victims was the email
marketing firm Epsilon, a unit of Alliance Data Systems Corp.

- On February 25, 2015, the US Senate Committee on Commerce, Science, and Transportation held a hearing on "Preserving the Multistakeholder Model of Internet Governance," during which it heard testimony regarding the Internet Assigned Numbers Authority (IANA) Stewardship Transition and enhancing the Internet Corporation for Assigned Names and Numbers (ICANN) accountability processes that have commanded significant attention of the global Internet community over the last year. If you are interested in reviewing the full hearing, an archived webcast is available here. More information about the Senate Committee is available here, and a July 31, 2014, letter from Senators Thune and Rubio (members of the Committee) to ICANN opining on the transition process and more generally on ICANN accountability is available here.

---

**Pharmaceuticals**

- The U.S. Food and Drug Administration launched the agency’s first mobile application (app) specifically designed to speed public access to valuable information about drug shortages. The app identifies current drug shortages, resolved shortages and discontinuations of drug products.

- China plans to lift price controls on pharmaceuticals in a move that could further open up a market that last year totaled about $105 billion, a 14% rise, but pricing pressure on drug makers may remain high.

- Merck is eliminating the 120-employee drug discovery department at Cubist Pharmaceuticals, which it recently purchased for $9.5 billion.

- Roche faces a class action lawsuit filed by Nutley, N.J., residents who claim the drug maker was negligent in handling hazardous chemicals that contaminated land below homes in their neighborhood and decreased property values.

- The U.S. Securities and Exchange Commission’s top enforcement chief warns that too many drug makers fail to accurately portray their dealings with the FDA.

- Health Canada is ramping up inspections of pharmaceutical manufacturing plants and will be publishing its findings online, and the regulator also told companies that it intends to increase “the frequency of planned and unplanned” inspections of facilities, according to The Star. The Star investigation revealed that FDA inspectors have found extensive problems at Canadian drug companies.

---

**Retail**

- New point-of-sale malware, LogPOS, has been using technology that evades detection by allowing the malware to inject code and act like a client while it shuttles stolen credit card numbers off to its command and control server. The technology, Microsoft Windows’ mailslots, isn't new by any means but it is the first time a POS malware variant has been spotted using it. Mailslots is an inter-process communications mechanism that allows multiple clients to send messages.

- Mandarin Oriental Hotel Group confirmed March 4 that the company is investigating a potential malware infection that breached the point-of-sale (PoS) systems in some of the chain’s 24 locations worldwide, including hotels in the U.S., which impacted an unknown number of customers. The investigation was initiated after financial institutions reported a pattern of fraudulent charges on payment cards used at Mandarin hotels dating back to December 2014.

- The National Consumers League, a nonprofit advocacy group is asking Congress to
urge retailers and other online businesses to purchase insurance that provides consumers with a safety net if criminals steal consumers’ personal information online. The group published its cybersecurity policy agenda after an annual Federal Trade Commission report showed that consumers and local law enforcement groups filed more than 332,000 complaints about identity theft last year.

- CNN Money reported that Costco has reached an agreement with Citi for a new co-branded credit card program, shortly after dropping its similar deal with American Express. Most retailers who accept Visa also accept MasterCard (MA), but Costco will be an exception to that rule. The only credit cards it will accept for store and gas station purchases will be Visa.

- Market Watch reported that shares of Lumber Liquidators Holdings Inc. fell sharply Monday, after a “60 Minutes” report alleged the U.S. retailer of hardwood flooring has installed Chinese-made laminate flooring in many American homes that contains far higher-than-accepted levels of formaldehyde, a chemical known to cause cancer.

- Yahoo News reported that the American Pet Products Association's annual report on pet industry spending says Americans spent $58 billion in 2014 on their 397 million pets, which range from freshwater fish and reptiles to cats and dogs. The industry trade group released the survey Thursday at the Global Pet Expo, an annual trade show in Orlando, Florida. The data came from a variety of groups, market research studies and media reports.

---

**Technology**

- It didn’t take long for fraud to find its way to Apple Pay. Some banks are seeing a growing incidence of fraud on Apple’s mobile-payment service as criminals exploit vulnerabilities in the verification process of adding a credit card, according to people familiar with the matter.

- A female developer at the heart of a debate over sexism in gaming has a message for those gathered at a prominent industry conference this week: you’re not doing enough to combat misogyny.

- ASML, a Netherlands-based machine manufacturing company for integrated circuits have been breached. The company stats that it hasn’t determined the identity of the attackers, but anonymous sources have cited that the attack was carried out by Chinese government.

- Virtualization software maker VMware is facing a lawsuit alleging that it has been violating the GPLv2 free software license for years with its use of Linux and other source code in ESXi. The case centers on “a combined work that VMware allegedly created by combining their own code (‘vmkernel’) with portions of Linux’s code, which was licensed only under GPLv2.”

- Recent sources have reported on a recent vulnerability, CVE-2015-0204 known as the Factoring RSA Export Keys (FREAK) vulnerability. The attack deliberately targets weak export cipher suites.

- Fake Flash Player Pro update delivers password-stealing Trojan. This campaign is targeting users who's DNS server settings have been changed to redirect them to malicious sites without their knowledge. This can be the result of a previous compromise of their routers via malware such as the DNSChanger Trojan, or a malvertising campaign.

- Angler Exploit Kit has been utilizing a “new technique” to evade detection whilst carrying out its malicious activities. Cisco has dubbed this technique as “domain shadowing” which involves compromised domain registration accounts. The attackers would hijack the accounts, usually thru phishing, and then use them to create subdomains.
Telecommunications

- A group of hackers calling themselves Team Hans managed to gain access to corporate information belonging to Canadian telecommunication and media company Rogers Communications relying mostly on their charm. The dump is over 400MB in size and contains contracts with corporate customers, business emails, sensitive employee information (ID, documents), as well as credentials for the VPN (virtual private network), which would allow access to the internal computer infrastructure of the company.

- Mark Zuckerberg is trying to mend fences with the telecom industry. Facing criticism from carriers that say Facebook Inc. is hurting their business models, Mr. Zuckerberg struck a conciliatory tone Monday, saying the only way to expand Internet access around the world is if carriers’ revenue grows too. “It’s really important not to lose sight of the fact that the real companies that are driving this are the operators,” the Facebook CEO said at the telecommunications industry’s main annual conference in Barcelona.

- In his keynote at the GSMA Mobile World Congress in Barcelona, Spain, Federal Communications Commission Chairman Tom Wheeler said for the first time mobile, or wireless Internet, will be covered in the new net neutrality rules approved late last month by the FCC. He also defended the rules, disputing claims that net neutrality stifles a free and wide open Internet.

Defense

- Significant security weaknesses in the Federal Aviation Administration’s information security program have placed the nation’s air traffic control system at risk of being hacked, according to a Government Accountability Office audit report.

- International Association of Machinists and Aerospace Workers (IAMAW) and Lockheed Martin subcontractor AllSource Global Management have reached a tentative labour deal brokered by federal mediators, the Federal Mediation and Conciliation Service announced on 2 March. The deal covers IAMAW local 219's workers, who have been on strike since 1 October from providing services for US Army Special Forces out of Lexington, Kentucky.

- U.K. politicians are calling for the tracking of leisure and commercial drone flights to avoid having safety concerns stifle an industry considered to have huge potential for job creation. Members of the House of Lords, the Parliament’s upper house, said in a report released Thursday that drones should be tracked and traced, especially those flying below 500 feet, to help keep air routes safe and help enforce rules on the use of such unmanned aircraft.

- Iran unveiled that a new, long-range surface-launched land attack cruise missile. The missile is called “Soumar” was presented to the Iranian Defense Minister. Unveiling the missile developed by Iranian scientists Dehqan said the new weapon ‘will increase Iran’s deterrence might’.

- MLSTONES (model for identifying cyber-threats) leverages technologies and methods from biology and DNA research, have effectively mapped a solution to flexibly represent and identify signatures and express them in a biology-based language that cannot be “translated” back to the original data. The LINEBACKER tool would apply to the methodology to discover malicious sequences of traffic in computer networks.
CIA Director John Brennan has ordered a sweeping reorganization of the agency, an overhaul designed to make its leaders more accountable and close espionage gaps amid widespread concerns about the spy agency's limited insights into a series of major global developments. Brennan announced the restructuring to the CIA workforce on Friday, including a new directorate devoted to boosting the CIA's computer hacking skills. He said the move comes after nine agency officers spent three months analyzing its management structure, including what deputy CIA director David Cohen called "pain points," organizational areas where the CIA's bureaucracy does not work efficiently.

Two security screeners at San Francisco International Airport have been charged with accepting bribes in exchange for allowing smugglers to carry methamphetamine through an airport checkpoint. According to the federal complaint, Claudio Rene Sunux, 30, of San Francisco, and Amanda Lopez, 27 of South San Francisco, were security screeners contracted with the TSA when they allowed alleged drug smuggler, 28-year-old Anibal Giovanni Ramirez to pass through security with drugs in the carry-on luggage.

The FBI is investigating the hacking of several business websites in the U.S. that showed a black ISIS flag on the homepage. NBC News reports that the home pages showed the words, "hacked by ISIS, we are everywhere," with a link to a Facebook page that doesn't exist. What appeared to be an Arabic song played in the background. The targets included Eldora Speedway in Rossburg, Ohio, owned by NASCAR star Tony Stewart, and a Goodwill center in St. Louis, among others.

A Secret Service agent and sheriff's deputy were allegedly assaulted while investigating threatening tweets against President Obama. A 19-year-old Clark County, Ohio man was arrested at his home after being alerted to online threats against Obama, police and other politicians. When the deputy and agent approached Ronald E. Skelton II, on his driveway, Skelton allegedly became "belligerent" and defiant, making antigovernment comments. He is accused of punching a detective and agent in the head, causing serious injury, while they tried to check him for weapons.

The boost in oil production in North Dakota has brought a lot of wealth – and crime – to the state. The FBI is responding to an uptick in crime by opening an office in the state's oil country. The bureau plans to fully staff the Williston office later this year, which will be a "resident agency" of the FBI's Minneapolis division.

A long-awaited report on Ferguson found numerous constitutional violations that called for new oversight, retraining of employees and abandoning the current approach to policing. The New York Times reports that the Justice Department criticized Ferguson police for routinely making unlawful searches, hurling racial insults and treating anyone as a criminal for questioning the tactics. While a separate report found no civil rights abuses against the white officer who shot and killed Michael Brown, an unarmed 18-year-old, the Justice Department described a discriminatory environment that led to months of protests.

The FBI arrested a man accused of at least five shootings in the Baltimore and Washington D.C. area over the past two weeks. The New York Daily News reports that the suspect, whose name has not yet been released, also shot up the NSA building Tuesday.