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

2015 Security Trends Webinars

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

Dates: February 24, 25, & 26

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

Top Incidents

**Energy**

- The United Steelworkers union, representing workers at about two-thirds of U.S. oil refineries, is issuing strike notices after rejecting a fourth contract proposed by Royal Dutch Shell Plc on behalf of energy companies. The steelworkers’ national agreement with Shell, Exxon Mobil Corp. and other refiners expired. The union hasn’t called a strike and is notifying local management “so preparations can be made” should one occur, union spokeswoman Lynne Hancock said. The USW described Shell’s latest
Agribusiness

- The Columbus Dispatch reported that J.M. Smucker Co. is buying pet food maker Big Heart Pet Brands in a $3.2 billion cash-and-stock deal, giving it a presence in the fast-growing $21 billion pet food industry.

Insurance/Healthcare

- Health insurer Anthem Inc. has suffered a massive data breach after hackers gained access to a corporate database reportedly containing personal information on as many as 80 million of the health insurer's current and former U.S. customers and employees.

Financial Services

- A US security firm claimed that it has evidence that Russian hackers have been silently siphoning off information from a major Japanese-owned Hollywood film company for the last few months, and they may even be the ones responsible for the catastrophic attacks in November, which the US blamed on North Korea. The firm also claimed that it's highly likely that the Russians still have access to the company's network.

Global Intelligence

- A posting on Udn.com reports several Chinese online retail websites suffered security breaches and exposed customer information. According to the posting, a criminal group has been using the exposed information to con retail websites customers.

Legal and Regulations

- The Federal Communications Commission (FCC) is taking a fresh look at its definition of a multi-channel video programming distributor (MVPD). In the past, it was easy to identify an MVPD. With limited exceptions, it was either a cable or satellite service provider. However, with the wide-scale accessibility of broadband networks, video capable-devices, video programming distributors and facility-based IP networks, there are now many options for "broadcasting" video programming. The FCC's Notice of Proposed Rulemaking (NPRM) seeks comment on whether any new or emerging video programming providers, such as Netflix, Amazon Prime, Roku and Apple TV, should be defined as an MVPD and, if so, what rights and obligations currently imposed on MVPDs should be extended to these new services and their providers.

Pharmaceuticals

- Following a four-week trial, a California man was found guilty in New York on all seven counts in connection with his operation and ownership of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs and other unlawful goods and services anonymously and beyond the reach of law enforcement.

Retail

- New York Times Dealbook reported that RadioShack has filed for Chapter 11 bankruptcy after striking a deal to sell up to 2,400 of its stores to Sprint and a hedge fund that is its biggest shareholder.

Technology

- The Chinese government recently implemented regulations that would require backdoors in foreign hardware and software. It would mandate that foreign companies that sell computer equipment to Chinese banks to disclose source code, submit to audits and build backdoors into both hardware and software.

Telecommunications
Democratic senators on Friday called on federal regulators to investigate Verizon Wireless, the country's biggest mobile provider, for secretly inserting unique tracking codes into the Web traffic of its some 100 million customers. Data privacy experts have accused Verizon of violating consumers' privacy by using "supercookies," an identifying string of letters and numbers attached to each site visited on a person's mobile device.

**Defense**

- An extensive and sophisticated cyber espionage operation targeting mainly Western military, government, defense industry firms, and the media, now has a new weapon: a spyware app for Apple iPhones and iPads. Operation Pawn Storm, which has been tied to Russia by at least one security research firm, is using a specially crafted iOS app to surreptitiously steal from the mobile device text messages, contact lists, pictures, geo-location information, WiFi status of the device, lists of installed apps and processes -- and to record voice conversations, according to new Trend Micro research.

**Law Enforcement**

- A license-plate scanning system designed to combat drug trafficking and other crimes has raised serious privacy questions because of the technology's ability to snap photographs of drivers and their passengers, the ACLU recently said. The concern is that authorities will combine the photographs with facial-recognition software.

**Energy**

- An activist with the group, Stopping Extraction and Exports Destruction (SEED), climbed a 150 foot crane at a Dominion construction site that is part of the Cove Point liquefied natural gas export terminal project. She hung a banner reading, "Dominion get out. Don't frack Maryland. No gas exports. Save Cove Point." The Maryland school teacher was arrested and released the statement, "The Dominion Cove Point LNG project is negatively impacting the environment and community in Lusby, MD. We are already seeing that it will directly lead to massive expansion of natural gas drilling and infrastructure throughout the mid-Atlantic region, from the coast to the Appalachian Mountains. I'm taking direct action today because I'm not willing to let the natural gas industry destroy Maryland, my home."

- Over 100 environmental and community groups are taking part in a protest in Oakland CA, the hometown of Governor Jerry Brown. Thousands of people marched in opposition to "fracking" and organizers called it the largest anti-fracking protest in the United States having bused in protesters from around the state. Demonstrators called on California Gov. Jerry Brown to place a ban on fracking, citing concerns over pollution, poisoning of water supplies and climate change. A day earlier, 12 people were arrested as protesters blocked the entrance to Brown's San Francisco office and erected a 16-foot fracking rig in the middle of an intersection.

- A group of Ottawa environmentalists interrupted a presentation given by TransCanada Corp.'s Energy East pipeline president François Poirier at the Château Laurier on Monday. Poirier was due to speak at 12:50 p.m., but had barely taken the podium at the luncheon meeting of the Canadian Club of Ottawa when four members of Ecology Ottawa walked to the front of the room and silently unrolled long banners protesting the pipeline. The banners read, "We can't drink oil!" and "Stop Energy East!" Two other pipeline opponents remained in the audience and photographed the protest. The Ecology Ottawa members paid $75 each to enter the event. The banners were small enough that they could be rolled up and stuffed in the arms of coats that were carried into the dining room at the hotel. The protesters were escorted out by hotel security guards. No charges were laid. For Ben Powless, a pipeline community organizer with the Ottawa group, the demonstration was meant to remind TransCanada of the stiff opposition the pipeline faces.
• Environmentalist groups are providing support to some striking oil workers, highlighting recent efforts to unite labor and environmental activism in the United States.

• Greenpeace in Colorado is planning to protest at Resource Capital Funds a Denver-based financial firm on Global Divestment Day, February 13.

• An article posted on Rabble.ca discusses several strategies to stop pipeline constructions or expansions. The author criticizes each one and eventually decides that 'Plan D' is the best way to achieve the desired end. Plan D is described as follows - What if logistical support, reinforcements and funding for legal challenges poured in from around the province and across the country? What if the unions who have come out against the pipelines sent people to stand with First Nations protecting the land? And what if those unions backed up their members with the threat -- and maybe the reality -- of industrial action if they were attacked? What if we don't allow ourselves to be divided over tactical differences; who is too radical, who is too moderate, who looks scary with a bandana over their face, who is wearing a suit and tie? What if we actually stand together across all the differences of age and politics and styles to defend the land, the waters -- indeed all life on this fragile and beautiful planet? That is Plan D. Plan D is a strategic plan that can actually stop the pipelines. In fact it is the only one that can. You might say that would be fine if publishing this piece had not given away the element of surprise. Except the other side has always known about this plan, indeed it is the only one they are really afraid of. That is why we can be confident it is the winning strategy.

• CBC has reported that what started as a forum teaching children about potential careers in LNG in Kamloops, B.C. was turned into a protest by several local anti-fracking demonstrators on Tuesday. About a dozen protesters from the Secwepemc Women Warrior Society and The Caretakers burst into the auditorium where the forum was being hosted by the province, WorkBC and Science World. They were waving signs reading “Fracking endangers humanity.” “We went to intervene and let the children know that they have choices,” said Kanahus Manuel, one of protesters. “Whether it is clean water or indigenous land rights, they have choices on where their position is going to be as the future.” The protesters were eventually forced from the conference by RCMP officers.

• The Albuquerque Journal News discusses a report by the federal Department of Energy’s Office of Inspector General. According to senior lab officials, an important error occurred when the note-taker at a meeting mistakenly wrote down “an organic” instead of “inorganic.” The mistake was compounded by a failure to catch it in subsequent reviews, the LANL officials said. The Inspector General’s report on how a waste drum from LANL popped open and contaminated the nation’s repository for certain types of nuclear waste says the errors likely would have been discovered if an appropriate “subject matter expert” at LANL had reviewed procedural changes. Those revisions led to the addition of organic, wheat-based cat litter into radioactive waste barrels containing nitrate salts -- essentially, the recipe for an explosive. The senior LANL officials who talked to the Journal said that no high-level scientist with sufficient expertise was ever involved in the procedural review.

• Several coal companies working with the government on the long-planned $1.65 billion FutureGen clean-coal project said Tuesday they have no choice but to shut it down after the Department of Energy suspended the majority of its funding, the Associated Press reports. “The department confirmed that it will not provide the $1 billion in stimulus funding it had committed to the project, which aimed to refit a coal-fired power plant near Meredosia in western Illinois and store carbon dioxide from the coal underground.

• Public opposition to onshore wind farms in the UK has fallen to a three year low of just 10 per cent, according to new government survey today that casts doubt over David Cameron’s claim that people are “fed up” with the technology.

• The Welsh parliament has voted against the use of shale gas fracking in Wales, just one week after Scotland passed a fracking moratorium, highlighting growing discontent with the British government’s push to tap shale gas resources.
Gov. John Hickenlooper’s (CO) task force on oil and gas discussed proposals Monday that would force energy companies to disclose all the chemicals they use in hydraulic fracturing and give local governments more of a say on where wells can be drilled.

Last month an anti-fracking group settled a lawsuit against Pennsylvania, after it was erroneously labeled a potential terrorist threat. The case dates back to 2010 and was an embarrassment for then-Governor Ed Rendell. But documents obtained by StatelImpact Pennsylvania show law enforcement here and in other parts of the country continue to conduct surveillance on anti-fracking activists, leading some to claim their Constitutional rights are being violated.

The United Steelworkers union, representing workers at about two-thirds of U.S. oil refineries, is issuing strike notices after rejecting a fourth contract proposed by Royal Dutch Shell Plc on behalf of energy companies. The steelworkers’ national agreement with Shell, Exxon Mobil Corp. and other refiners expired. The union hasn’t called a strike and is notifying local management “so preparations can be made” should one occur, union spokeswoman Lynne Hancock said. The USW described Shell’s latest proposal in a telephone message as “insulting” and instructed all local units to reject it.

Agribusiness

- GMO-labeling bill HB 92 has been introduced in Alaska by Representatives Geran Tarr and Scott Kawasaki. The bill would also prohibit labeling a product as “natural” if any GM products were included in its production.

- The government of Denmark announced plans to double national organic agriculture by 2020 and to increase the amount of organics served in meals in public institutions to 60%.

- On February 1, Sustainable Pulse reported on the growing global opposition to the approval of GM loblolly pines with minimal oversight and scientific study. This outrage from the public and scientific community comes after the USDA agreed to allow ArborGen to cultivate these trees commercially with virtually no regulation. Pollen from loblolly pines is known to be able to drift for hundreds of miles.

- The peer-reviewed journal, Environmental Sciences Europe, has published a statement asserting there is no clear consensus on the safety of GM products and crops. The statement has been signed by over 300 scientists and experts from relevant fields. By publishing this statement, it is now a citable source making up part of the body of peer-reviewed scientific literature.

- IOI Corporation has officially committed to sourcing palm oil that is not connected with deforestation and human rights abuses. IOI Corporation made this announcement that it will comply with the pledge previously made by its subsidiary, IOI Loders Croklaan. According to experts, over 90% of the world’s palm oil is connected to some sort of zero-deforestation commitment.

- The Center for Food Safety released a report about the dramatically declining Monarch Butterfly population related to herbicide use in the Midwest responsible for destroying the Monarchs’ primary food source, milkweed. A presentation is being given by CFS to Congress today to go over the major points of this 80-page scientific report.

- A blogger, calling herself “Food Babe” has been campaigning for cereal makers to cut butylated hydroxytoluene (BHT) from cereals. General Mills claims it began working to remove BHT from cereals more than a year ago, before Food Babe began campaigning.

- USA Today reported that Coca-Cola announced that its Minute Made division is beginning to sell a premium-priced, protein-boosted milk under the Fairlife label. It will be available nationally next month when a national ad campaign breaks.
• Battle Creek Enquirer reported that The Kellogg Co. said it will have “no choice” but to close at least one U.S. cereal plant in the “very near future” if employees don’t reconsider proposed contract changes they rejected two months ago. The Battle Creek-based company did not say which plants would be shut down.

• The Columbus Dispatch reported that J.M. Smucker Co. is buying pet food maker Big Heart Pet Brands in a $3.2 billion cash-and-stock deal, giving it a presence in the fast-growing $21 billion pet food industry.

Insurance/Healthcare

• As of February 3, the Maryland General Assembly updated Bill 790, making Maryland the first state to provide patients a form ensuring confidentiality. It allows for patients to have their medical bill sent to another address that doesn’t belong to the policy holder.

• Health insurer Anthem Inc. has suffered a massive data breach after hackers gained access to a corporate database reportedly containing personal information on as many as 80 million of the health insurer’s current and former U.S. customers and employees.

• Massachusetts' UMass Memorial Medical Group (UMMMG) recently acknowledged that a former employee may have inappropriately accessed patient information; approximately 14,000 patients may be affected.

• The Obama administration’s proposed fiscal 2016 budget calls for increases in funding for the HIPAA compliance audit program as well as the development of nationwide secure health data exchange. It also would provide funds for the removal of Social Security numbers from Medicare cards in an effort to reduce ID theft.

• Over the past few weeks, several hospitals and medical centers have announced that stolen devices, including computers, laptops and mobile phones, exposed thousands of patients’ personal information. It’s an ongoing problem that doesn’t show any signs of slowing down, despite growing awareness of the importance of encryption.

• Federal regulators are on the right track in their vision for a "roadmap" to remove barriers to nationwide, secure health information exchange, but many more hurdles remain, security and privacy experts say.

• Senior Health Partners (SHP), a Healthfirst company, recently notified approximately 2,700 of its members that a laptop and smartphone belonging to an assessment nurse employed by Premier Home Health ("Premier"), a business associate, were stolen from the nurse’s apartment. SHP and Premier conducted investigations and found no indication that anyone accessed or misused any personal information or protected health information. Nevertheless, SHP is notifying members so they may protect themselves.

• Breaches can happen even when there are strong protections in place. But healthcare organizations can do more to prepare for breaches and respond in the best possible way to protect patient information. Three tips to avoid common pitfalls in healthcare incident response programs are: 1) define incidents broadly; 2) teach the workforce to report incidents; and 3) make a comprehensive incident response plan.

• The Information Commissioner has welcomed a change in the law that will give his office the right to force NHS authorities to be audited for compliance with the Data Protection Act. From February 1st, the ICO will be able to subject public healthcare organizations to a compulsory audit. These compulsory audits have previously only applied to central government departments.

• The National Association of Insurance Commissioners has created a new task force that will be focused on cyber security. The task force is meant to increase consumer protection, introducing new regulations that target the insurance industry. Insurers collect valuable information from their customers, but new risks are emerging in the
digital world that put this information in danger of theft and exploitation. The new task force could help foster further innovation in the world of cyber insurance.

### Financial

#### Financial Services

#### Activism

- Housing activists are planning to stage an anti-eviction blockade in support of a local family facing eviction from their bank-owned home in Chicago, IL.

- Activists called for the occupation of an insurance conference organized by a leading U.S. financial institution on February 12 in NYC.

- Australian union workers will conduct anti-government rallies in all of Australia’s capital cities on March 4 in response to the Abbott administration’s Productivity Commission inquiry into workers’ rights.

- A coalition of Indian banking unions announced that public sector bank employees may go on a four-day strike beginning February 25 if their demand of a 19% wage increase is not met.

- Housing activists from Barcelona, Spain are planning protest actions on February 11 in New York City and San Francisco, CA to protest global speculation in the housing market. The event in New York City, will take place at 12:30 PM EST in front of the firm’s office building on Park Avenue. The event in San Francisco, CA will occur at 8:00 AM PST in front of the office of an American multinational private equity and investment firm located downtown.

- The FBI ordered numerous banks in the Washington, DC area to close their doors temporarily on February 2 due to a bomb threat. The FBI’s Washington field office received a call February 1 from the Netherlands via a Canadian telephone operator in which the caller said the bomb would detonate at a national bank in the center of Washington at noon on February 2. The call was determined to be a hoax.

#### Information Security Risk

- An emerging malware downloader dubbed ‘F0xy’ employs various evasion techniques and downloads a cryptocurrency miner. ‘F0xy’ is able to dynamically change its command-and-control (C&C), download and execute arbitrary files. The malware employs very little in the way of code and string obfuscation in order to appear more legitimate and hide in plain sight. It also uses Microsoft’s Background Intelligent Transfer service to outsource its network traffic in order to avoid detection from security products.

- A third vulnerability in Adobe’s Flash Player was discovered since the beginning of the New Year and is being actively used to attack visitors to a popular video-sharing website. Researchers said hackers are actively exploiting it to carry out malvertising campaigns, with visitors to the website redirected through a series of other websites until landing on the URL where the exploit is hosted.

- A serious security flaw in Internet Explorer could be exploited by malicious hackers to launch convincing phishing attacks and inject malicious code into users’ browsers as they visit websites. The bug, which works on Internet Explorer 11 running Windows 7 or Windows 8.1, is a universal cross-site scripting (XSS) vulnerability, and bypasses what is known as the Same-Origin Policy.

- An Android banking Trojan with a very low antivirus detection rate is targeting Chinese mobile users. This Android malware is capable of stealing banking information by intercepting SMS messages looking for certain keywords. It also steals all the contact...
information from the user’s mobile device and relays it to a remote Command & Control (C2) server.

- The Financial Industry Regulatory Authority released a report on February 3 that surveyed 20 brokerage firms and found that the threat of an online intrusion by a nation or a terrorist group ranked near the bottom of the industry’s concerns. Worries about state-sponsored breaches were highest at big investment banks. Few of the largest firms questioned by FINRA put such attacks at the top of their list. All the firms said they had little concern about a hacking breach carried out by a competitor. The report said about 80 percent of firms questioned already conducted some form of periodic security self-assessment. But the regulatory agency said it was “concerned that the remaining firms either had no program in place or were in the nascent stages of establishing a program.”

- The Securities and Exchange Commission issued its own report on February 3 that examined how prepared Wall Street investment banks and brokerage firms were to repel hackers intent on gaining access to their digital networks. That examination of more than 100 registered firms found that the overwhelming majority “have been the subject of a cyber-related incident.” The most common attacks involved hackers introducing malware into a firm’s network or the use of fraudulent emails seeking to persuade brokers to improperly transfer a client’s money.

- A US security firm claimed that it has evidence that Russian hackers have been silently siphoning off information from a major Japanese-owned Hollywood film company for the last few months, and they may even be the ones responsible for the catastrophic attacks in November, which the US blamed on North Korea. The firm also claimed that it’s highly likely that the Russians still have access to the company’s network.

- An online parking reservation service for airports across the United States suffered a data breach losing an unspecified number of payment card information. Investigators said the hack was carried out by the same hacker gang that stole more than a 100 million credit and debit cards last year from the Minnesota-based national retail store and the home improvement store headquartered in Florida. The parking service company is the third online parking service since December 2014 to fall victim to this cybercriminal group.

- For the second time in 12 months, multiple financial institutions complained of fraud on customer credit and debit cards that were all recently used at a string of hospitality facilities run by a Merrillville, Indiana-based hotel franchise firm. Banking sources said the cards that were compromised in this most recent incident appear to have been stolen from many of the same locations implicated in the January, 2014 breach, including hotels in Austin, Texas, Bedford Park, Ill., Denver, Indianapolis, and Louisville, Kentucky. Those same sources said the compromises appear once again to be tied to hacked cash registers at food and beverage establishments within the hotels managed by the firm. The legitimate hotel transactions that predated fraudulent card charges elsewhere range from mid-September 2014 to January 2015.

**Legal, Litigation, Regulatory Risk**

- A Romanian man pleaded guilty to charges stemming from his role in a large-scale ATM skimming scheme that defrauded several leading U.S. banks out of at least $5 million. Authorities said the ATM skimming operation is one of the largest ever uncovered by law enforcement. The ATM skimming scheme targeted thousands of bank customers throughout New Jersey, New York, Connecticut, Florida and elsewhere, authorities said. The accused and his co-conspirators constructed sophisticated card-reader devices capable of reading and storing customers’ bank account information as the customers performed routine banking transactions at ATMs. The conspirators also hid pinhole cameras in panels designed to match existing ATM components. The accused then taught and directed several conspirators to install the devices on ATMs. Once installed, the card-reader devices secretly read identity and account information contained on the magnetic strip of customer ATM cards. The pinhole cameras recorded customer keystrokes as they entered their personal
identification numbers. After stealing the information, the gang created thousands of fraudulent ATM cards, which they used to withdraw millions of dollars from customers' bank accounts.

- A leading U.S. bank agreed to pay $18 million to former customers of an Iowa-based financial firm that shut down in July 2012 to resolve claims that the bank aided a massive fraud by the failed futures brokerage's now-imprisoned founder.

- A UK-based voice and electronic dealer broker and provider of post trade risk services agreed to pay a $17 million fine for breaking EU antitrust rules by helping to manipulate the yen benchmark interest rate, the European Commission said last week. The fine levied on the company follows a massive probe by EU regulators into banking-industry practices in the wake of the worldwide financial meltdown. In this case, involving Japanese yen interest rate derivatives, the commission uncovered seven bilateral agreements between banks to fix the London interbank offered rate, or Libor, as it was tied to the yen.

- A major American insurance company agreed to settle a 2011 lawsuit accusing a leading U.S. investment firm of fraud over more than $100 million worth of mortgage-backed securities in which the insurer invested. The largest publicly traded U.S. home and auto insurer sued the investment firm and other lenders in 2011, alleging they sold packages of risky home loans while claiming they conformed with “conservative” underwriting standards. A Northbrook, Illinois-based insurer and New York-based investment services firm have agreed to discontinue the suit, according to a February 2nd court filing in New York State Supreme Court.

**Operational Risk**

- An op-ed published by a leading conservative news agency said that President Obama's announcement of lowering the insurance premium for risky FHA mortgages will take the country back to the same policies that created the 2008 financial crisis. The piece claimed that a cut in the FHA insurance premium is putting taxpayers and homeowners at risk because if mortgages fail once again, they will drive down housing prices in every neighborhood and every family in those neighborhoods could suffer a loss in the value of their homes.

- The Crimean Prime Minister announced that an alternative to two of the most widely used American credit card services will be working in Crimea by May 1 of this year, the traditional start of tourist season in Russia. He claims that the mechanisms for the new payment system already exist and are now being tested.

- An activist group whose goal is to end extreme poverty by 2030 initiated a campaign that demands finance ministers and world leaders commit at least 30% of the new financial transaction tax to development, social infrastructure and to crucial areas like health, education, youth employment, climate and safety.

**Reputational Risk**

- Leading U.S. investment firms are being accused of attempting to hide their alleged practices of paying executives multimillion-dollar awards for entering government service. Reportedly, three leading U.S. investment firms delivered a letter to the SEC seeking exemption from a shareholder proposal by the AFL-CIO, which would force the firm to identify all executives eligible for these financial rewards and the specific dollar amounts at stake.

- A leading U.S. bank is being accused of hiding racial criteria to steer first-time home buyers into certain neighborhoods and particular lending programs, according to a housing group that sent women of various races to apply for loans. The nonprofit housing group sued the bank in Manhattan federal court on February 3, seeking an order prohibiting the discriminatory practices, requiring the training of employees and allowing for the monitoring of the residential lending process as well as unspecified money damages.