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

Join Our Webcast on April 24
In this webinar we'll look at how you can use an individual's online “footprint” to identify potential threats and develop a more effective security plan.

Top Incidents

Energy

- ExxonMobil, the nation’s largest oil and gas company, will begin disclosing risks associated with shale drilling and fracking to investors, in response to a long-running campaign by a coalition of shareholders. Exxon will publish a report by September that will describe fracking's potential harm to air quality, water and roads, as well as risks associated with the chemicals used. Exxon agreed to follow criteria identified in a 2013 report, cited by the coalition and called Disclosing the Facts: Transparency and Risk in Hydraulic Fracturing Operations, in which Exxon received a failing grade for its transparency.
Several sources report that biotechnology stocks have fallen 5.6% (WSJ), with some individual companies’ stocks falling as much as 23% (ABC, CBS). Activists have widely attributed this news to the “Operation Monsanto Stock Plunge” by Food Democracy Now!, in which participants hope to cause financial damage to agribusiness companies by withdrawing investments from mutual funds which include agribusiness stocks.

**Insurance/Healthcare**

- Many healthcare organizations need to improve their basic cybersecurity "blocking and tackling," and most also need to improve their willingness to share cyber-security information, says Kevin Charest, chief information security officer at the U.S. Department of Health and Human Services.

**Financial Services**

- Computer security experts are advising administrators to patch a severe flaw in OpenSSL versions 1.0.1 through 1.0.1f, with two exceptions: OpenSSL 1.0.0 branch and 0.9.8. The flaw, nicknamed “Heartbleed,” could allow attackers to monitor all information passed between a user and a Web service or even decrypt past traffic they’ve collected. The scope of the problem is vast, as many modern operating systems are suspected as having an affected OpenSSL version. Operating systems that may have a vulnerable version of OpenSSL include: Debian Wheezy, Ubuntu 12.04.4 LTS, CentOS 6.5, Fedora 18, OpenBSD 5.3, FreeBSD 8.4, NetBSD 5.0.2 and OpenSUSE 12.2.

**Worldwide Intelligence**

- Famed hacking group Anonymous has struck again with attacks on numerous websites operated by Israeli ministries and organizations in an effort labeled as “OpIsrael.” The attacks are in regards to the group’s disagreement with Israeli policies, which include those that affect Palestinian territories. Anonymous introduced “OpIsrael” in November 2012 during an Israeli assault on Gaza. During the initial attacks, some 700 Israeli websites were taken down.

**Energy**

- On Sunday April 5, coordinated anti-fracking protests in 60 Romanian cities called for a ban on hydraulic fracturing, transparency in decision making, and for the Romanian government to respect the will of local communities. The events followed months of protests beginning in Pungesti, a small village near the border with Moldova, but have spread as activists learned that fracking operations are planned or are already underway across Romania. Chevron is the main operator in the bloc.

- New regulations unveiled by the European Commission will affect renewable energy subsidies in the bloc. The move is an attempt to lower prices and boost competitiveness. The new rules were adopted by the European Commission in Brussels on Wednesday. A statement from the commission read that the guidelines “promote a gradual move to market-based support for renewable energy.” Currently in some EU nations, state subsidies are used to support certain renewable energy schemes, such as solar or wind power. Funding for the subsidies often comes in the form of higher prices for consumers and industries. Under the new rules, these subsidies would gradually end, and competitive bidding processes for allocating public support to renewable energy projects would be implemented in their place.

- A series of earthquakes over the April 3-5 weekend continued to break records of seismic activity in Oklahoma, which some scientists say is linked to increased fracking
operations in the state. According to Reuters, six earthquakes struck central Oklahoma between Friday afternoon and Saturday morning, including a 3.8 magnitude tremor that was recorded around 7:42 a.m. Prior to this quake, three others hit the area in multiple communities: one at a magnitude of 2.9, and two others at 2.6 and 2.5 magnitude.

- Pacific Gas & Electric Co. offered a $250,000 reward Thursday for information leading to an arrest and conviction in a startling attack mounted nearly a year ago on telephone lines and the power grid in Silicon Valley. PG&E’s reward would be funded by shareholders and comes nearly a year after AT&T offered its own $250,000 reward for information leading to arrests.

- The Nuclear Regulatory Commission (NRC) has denied a petition by Nuclear Information and Resource Service (NIRS) and 37 co-petitioners to make modest improvements in the NRC’s emergency planning regulations. As a result NIRS has posted a press release saying that the NRC has failed the American people.

- The destination of Japanese shipments of weapons-grade plutonium that will be taken in by the United States cannot be confirmed; but many are speculating the plutonium will eventually wind up at the Savannah River Site. President Barack Obama recently announced that the United States secured more than 700 pounds of the material from Japan. The administration considers the move a win, since securing nuclear materials has been a part of its plan for several years. Local officials are far from celebrating, though, since many speculate the material will end up at SRS. Keri Fulton from National Nuclear Security Administration public affairs said that information is unavailable for security reasons, and would not confirm where the shipments will be stored. Dispelling further rumors, Fulton added the new shipments are not part of the Mixed Oxide Fuel Fabrication, or MOX, agreement involving the facility under construction at SRS.

- According to the most recent energy flow charts released by Lawrence Livermore National Laboratory Americans used 2.3 quadrillion thermal units of energy more in 2013 than the previous year. The Laboratory also has released a companion chart illustrating the nation’s energy-related carbon dioxide emissions. Americans’ carbon dioxide emissions increased to 5,390 million metric tons, the first annual increase since 2010.

- The Department of Energy’s inspector general said that information about the U.S. electric grid's vulnerability to physical attacks should have been classified for national security reasons, and called on federal regulators to change the way they handle such material. As The Wall Street Journal reported earlier this year, the Federal Energy Regulatory Commission briefed many utility executives, congressional leaders, trade groups and government officials about an attack by gunmen on an electrical substation in California in April 2013. The briefings included results of a computer model suggesting that knocking out a small number of critical transmission substations could result in cascading blackouts across North America. Inspector general Gregory Friedman’s office said all this information “should have been classified and protected from release at the time it was created.” The alert recommended that the independent energy commission take immediate steps to secure the information and prevent further public release.

- Tribal communities, farmers and ranchers from along the Keystone XL pipeline route will ride into Washington on horseback April 22 for a five-day encampment to protect the climate, land, water and tribal rights threatened by the pipeline. The Center for Biological Diversity and allies will join the rally Sunday, April 26 to demand that President Obama reject Keystone once and for all.

- A multi-community climate protest is being organized in Montana for April 26th.

- Protesters obstructed railroad tracks in Montana yesterday, stopping an energy train.
and resulting in seven arrests.

- Direct actions are planned in the San Francisco Bay Area between Earth Day on April 22 and May 1st. The actions will focus on labor, immigration, and environmental issues. Actions may include sit-ins, tree sits, guerrilla gardening, pickets, marches, blockades, and strikes.

- Activists are increasingly focusing on energy trains in the Pacific Northwest, raising tensions in communities along rail lines.

- A new activist report, "Dirty Fuels, Clean Futures," calls for new coal valuations and for scrutiny of the royalty charges for coal extraction on public lands.

- The Colorado Department of Public Health and Environment (CDPHE) has called in an epidemiologist to investigate a recent spike in fetal abnormalities in Garfield County on Colorado's western slope. Stacey Gavrell, Director of Community Relations for Valley View Hospital in Glenwood Springs, said area prenatal care providers reported the increase in fetal abnormalities to the hospital, which then notified CDPHE. So far neither the hospital nor the state have released information about the numbers of cases reported, over what span of time, or the amount of the increase. Gavrell said it is too early to speculate on the causes of the spike in abnormalities. The report comes shortly after the February, 2014 publication in Environmental Health Perspectives of a study that found an association between the density of natural gas wells within a ten mile radius of expectant mothers' homes and the prevalence of fetal anomalies such as low birth weight and congenital heart defects in their infants.

- Violence and protests in Algeria have forced the presidential campaign team of Abdelaziz Bouteflika to call off a rally, as tensions run high over the ailing veteran's bid for a fourth term. Protesters on Saturday stormed the venue for Bouteflika's rally in the eastern Kabylie region, setting fire to his portrait, the AFP news agency reported. Television channels broadcast footage showing a crowd of about 250 chanting "Bouteflika out" outside a cultural centre in Bejaia, where the rally was to be held. Demonstrators also attacked the crew of Ennahar television, the channel's chief Anis Rahman told AFP, adding that four journalists were injured.

- ExxonMobil, the nation's largest oil and gas company, will begin disclosing risks associated with shale drilling and fracking to investors, in response to a long-running campaign by a coalition of shareholders. Exxon will publish a report by September that will describe fracking's potential harm to air quality, water and roads, as well as risks associated with the chemicals used. Exxon agreed to follow criteria identified in a 2013 report, cited by the coalition and called Disclosing the Facts: Transparency and Risk in Hydraulic Fracturing Operations, in which Exxon received a failing grade for its transparency.

- Coloradans for Local Control launched a 30 second TV ad today promoting the proposed ballot measure that would give citizens the ability to ban fracking in their communities. The TV ad asks, "Would you want to live here? Want your kids to play here? Next to a fracking rig? Fracking can occur just 501 feet from businesses, playgrounds, even your home, and right now you and your neighbors can’t stop it." The TV ad says that with local control over oil and gas drilling, Coloradans will have the tools "to protect your neighborhood" from fracking. The TV ads will air on Denver cable.

- Last week, U.S. Transportation Secretary Anthony Foxx told Congress that his agency is committed to pressuring the oil-by-rail industry to come up with a safer tank car design for unconventional oil. "My target date is as soon as possible," Foxx said, although he would not commit to a hard deadline for stricter standards when pressed by the Senate Appropriations committee.

- Mark Ruffalo has initiated a petition at MoveOn.org titled, "URGENT: Stop Congress
from Rubber-Stamping Fracked Gas Exports!” He claims: “The oil and gas industry is using the crisis in Ukraine as an excuse to pressure Congress to rubber stamp approval of liquefied natural gas (LNG) exports. But gas exports won’t help the situation in Eastern Europe. It’s just a ploy by the oil and gas industry to increase fracking and export U.S. fracked gas to the highest bidder abroad, while causing irreparable damage to our climate and to water, air and health here at home. Protect our communities and climate – not big oil and gas industry profits.”

Agribusiness

- Several sources report that biotechnology stocks have fallen 5.6% (WSJ), with some individual companies’ stocks falling as much as 23% (ABC, CBS). Activists have widely attributed this news to the “Operation Monsanto Stock Plunge” by Food Democracy Now!, in which participants hope to cause financial damage to agribusiness companies by withdrawing investments from mutual funds which include agribusiness stocks.

- The MST reports that throughout the month of April, student groups affiliated to the MST at as many as 50 universities will conduct a series of “debates, exhibitions of theater, films, visits to settlements and trade” in support of agricultural reform in Brazil.

Insurance

- The Michigan Department of Community Health (MDCH) recently announced that 2,595 people’s personal information may have been exposed when a laptop and flash drive were stolen from an employee of the State Long Term Care (LTC) Ombudsman’s Office on the evening of January 30, 2014 or the early morning of January 31, 2014.

- Food and Drug Administration (FDA), along with the Office of the National Coordinator for Health Information Technology (ONC) and the Federal Communications Commission (FCC) recently published their health IT report. The report, required under the Food and Drug Administration Safety and Innovation Act (FDASIA), contained proposed strategy and recommendations for a risk-based framework.

- Surgical information for more than 1,200 patients may have been compromised in February when an unknown person accessed a doctor’s Gmail account. Midwest Orthopaedics at Rush said in a news release that names and dates of birth for 1,256 patients could have been accessed, along with descriptions, dates and instructions for their surgeries.

- The New York Insurance Association is asking lawmakers to act and put an end to insurance fraud. Auto insurance companies have called upon the Legislature to adopt a zero tolerance stance on this lucrative behavior and stop multi-million dollar illegal enterprises that put New York families at personal and financial risk.

- The Obama administration has issued a policy statement that says businesses sharing cyberthreat information with one another are not violating antitrust laws.

- Insurance-fraud prosecutions in Maryland just became easier thanks to a bill clarifying legal venues in which prosecutors can bring fraud cases, according to the Coalition Against Insurance Fraud.
An Austin, Texas, nonprofit advocacy group for children with developmental disabilities, EveryChild, Inc., recently announced that it has informed 2,934 families of a potential data breach. Internal computers containing patients’ birthdates, Social Security numbers, Medicaid numbers, photos and other health information were stolen from its office.

Many healthcare organizations need to improve their basic cybersecurity “blocking and tackling,” and most also need to improve their willingness to share cybersecurity information, says Kevin Charest, chief information security officer at the U.S. Department of Health and Human Services.

The digitization of medical records is being pitched to the public as a way to revolutionize healthcare. But rapid technological innovation and lagging privacy laws are leaving patients – and their most sensitive information – vulnerable to exposure and abuse, especially in this age of “big data.” The Electronic Frontier Foundation (EFF) is launching a new medical privacy project to identify the emerging issues and to give advocates the information they need to fight for stronger protections for patients.

Heartbleed, the biggest bug to hit the Internet in years, is putting everyone’s data at risk, especially their medical and healthcare data. Codenomicon estimates that about 66% of all devices connected to the Internet could be attacked using Heartbleed. Other systems such as home healthcare systems used to communicate with insulin pumps and back-end systems, home healthcare networks, and even medical devices such as MRI machines could all be attacked through this bug. Given reports of the already shoddy state of healthcare cybersecurity, events like this should further highlight the importance of having healthcare IT maintain the highest possible standards.

The Kaiser Permanente Northern California Division of Research recently began notifying approximately 5,100 Kaiser Permanente members who had participated in research studies that malware found on a server on February 12, 2014, may have compromised their personal information.

Bank of America and QBE Insurance Corp have agreed to pay $228 million to settle claims that they engaged in a kickback scheme inflating the cost of insurance that homeowners were forced to buy, according to a court filing.

Many healthcare IT security professionals have adopted patient privacy philosophies that revolve around clinical staff and those who handle protected health information (PHI) treating the data as though it were their own. The growing need for this type of thinking was highlighted in a recent Journal of AHIMA article that takes a look at medical identity theft and highlights best practices.

Financial Activism

A rally for equal gender pay occurred April 8th in New York City as participants called for advocates to support women’s economic opportunities and pay equality.

An activist group calling for immigration reform concluded its U.S. nationwide bus tour on April 9th in Washington, D.C. with a rally and protest march to Congress. On April 4th, the group’s tour bus stopped to protest at multiple corporate facilities, to include some financial firms, who are donors to various political figures who oppose immigration reform.
An activist group protested outside a leading U.S. investment bank in Worcester, MA on April 10th claiming the bank is a “corporate tax cheat.” The group will also protest outside a branch of the bank in Boston, MA on April 12th.

A protest calling to stop U.S. aid in Egypt occurred April 11th at the U.S. Chamber of Commerce in Washington, D.C.

Occupy activists in San Francisco, CA will conduct a "week of actions for wages and defend worker centers from attack" from April 24th through April 30th. No further details are disclosed at this time.

Environmental activists will conduct an Earth Day Action Parade on April 19th in San Francisco's Financial District. Participants will speak out against topics including dirty fossil fuels, Keystone XL, fracking, and big oil refinery expansions.

Spanish activists on April 10th blocked the entrance to a dozen of branches of a Spanish bank in downtown Barcelona, Spain, which they accuse of not doing enough to prevent mortgage holders from losing their homes. The demonstrators argued that Spain's fifth-largest bank has shown very little will to renegotiate the terms of mortgages held by customers who have hit hard times.

Activists will protest dairy price fixing and global carbon trading at a leading mercantile exchange in Chicago, IL on April 18th.

**Information Security Risk**

- Security researchers discovered a botnet dubbed “Sandroid” targeting Android smartphone users who bank at financial institutions in the Middle East which comes bundled with Android apps made to look like mobile two-factor authentication modules for various banks.

- A new variant of the Zeus banking Trojan uses a legitimate digital signature to avoid detection from Web browsers and anti-virus systems. The variant includes the digital signature, a rootkit and a data-stealing malware component. A sample of the latest Zeus variant tried to trick the recipient into executing it by posing as an Internet Explorer document that included an icon similar to the Windows browser. Because the file is digitally signed with a valid certificate, it appears trustworthy at first glance. When executed, the malware downloads the rootkit and a program capable of stealing login credentials, credit card information and other data a person keys into a Web form. The rootkit prevents the malicious files from being deleted by either the computer user or AV software.

- Hacktivists from several countries launched a new DDoS campaign on April 7th against Israel, targeting primarily financial institutions and government agencies in the pro-Palestine campaign.

- Security researchers demonstrated that MPOS, an emerging technology that enables retailers to process card payments using mobile phones or tablets, can be compromised via multiple attack techniques using micro USBs, Bluetooth and a malicious programmable smartcard.

- Computer security experts are advising administrators to patch a severe flaw in OpenSSL versions 1.0.1 through 1.0.1f, with two exceptions: OpenSSL 1.0.0 branch and 0.9.8. The flaw, nicknamed “Heartbleed,” could allow attackers to monitor all information passed between a user and a Web service or even decrypt past traffic they’ve collected. The scope of the problem is vast, as many modern operating systems are suspected as having an affected OpenSSL version. Operating systems that may have a vulnerable version of OpenSSL include: Debian Wheezy, Ubuntu 12.04.4 LTS, CentOS 6.5, Fedora 18, OpenBSD 5.3, FreeBSD 8.4, NetBSD 5.0.2 and OpenSUSE 12.2.
According to a leading antivirus vendor, banks and other financial institutions may be forced to shut off access to their online banking systems for those still using Microsoft Windows XP, support for which comes to an end this week. The antivirus vendor says that from 2012 to 2013, detections of online banking malware more than doubled from 500,000 worldwide in 2012 to more than a million in 2013.

Researchers from a reverse engineering applications security firm demonstrated how hackers can use ‘method swizzling’ and a rogue application to compromise a user’s online banking and, consequently, steal and transfer money out of the account. Method swizzling is a feature of Apple’s Objective C runtime programming language, which is often used by iOS developers to exchange one method for another, making it useful for usage logging, performance, or even adding or augmenting features. In addition, method swizzling is often used in the jailbroken community for user interface (UI) tweaks, and changing gesture controls. Fortunately, this kind of attack is only viable if the device has been jailbroken.

A leading anti-virus vendor found evidence of numerous criminals developing their own version of the Tor peer-to-peer model. ZeroAccess is an example of this, where criminals developed their own protocol to communicate. Criminals’ use of peer-to-peer technology is troubling as it makes tracking and shutting down their cyber campaigns more complex. Researchers uncovered evidence in March suggesting criminals plan to release a new wave of advanced cyber-attack campaigns using the anonymizing Tor network.

A stack-based buffer overflow vulnerability in the qconnDoor service could lead to remote code execution on BlackBerry 10 smartphones. If the exploit works, the attacker can execute code with superuser rights, or terminate the qconnDoor service. A software update has been released to address the vulnerability which has the CVE-2014-1468 identifier. The flaw affects BlackBerry 10 OS versions earlier than 10.2.0.1055.

**Legal, Litigation, Regulatory Risk**

- Hackers who recently raided the credit card payment system of a large U.S. retailer belong to a sophisticated Russian syndicate that has stolen more than 160 million credit-card numbers from retailers over seven years. The Russian group is well known to U.S. authorities, who have indicted several members and linked it to pillaging more than 100 companies.

- Russia is urging companies to delist their shares from overseas stock exchanges and trade in Moscow in an effort to safeguard them as international sanctions mount against the country after its takeover of Crimea. Further, the Russian government is creating “attractive” conditions for companies that decide to re-register on OAO Moscow Exchange, and will itself push on with plans to sell state-owned assets on the stock exchange.

- A U.S. District Court judge sided with the Federal Trade Commission’s (FTC) attempt to punish companies for poor security standards that lead to data breaches, as it refused to dismiss the agency’s lawsuit against a hotel and resort chain for getting hacked. The FTC claims the company’s promise to protect users’ data was “unfair and deceptive.”

- The Consumer Financial Protection Bureau recently ordered a leading U.S. investment bank to repay $727 million to consumers wronged by the bank’s deceptive marketing practices regarding credit card add-on products.

- A U.S. university law school published a study that concludes minority residents in Minneapolis, MN are “much more likely than white people of similar incomes to be rejected for a mortgage, whether they’re buying a home or refinancing.” The study, using data from 2009 to 2012, focused more on general patterns than on particular
bank activity. But it notes the “two largest banks in Minnesota would have made an additional 5,400 mortgage loans in racially diverse and mostly non-white Twin Cities neighborhoods during that period if they had distributed their loans proportionally to the distribution of homeowners with various incomes across the region.”

**Operational Risk**

- Occupy Wall Street hosted an open coordination conference call on April 8th for the purpose of planning Worldwide Wave of Action disruptive events.

- A Bitcoin magazine source reports Virtex is soon launching a platform that will allow for the exchange of cryptocurrencies at an international level. The Virtex exchange platform was created using PHP Symfony 2, a reputable web development framework that allows for the creation of custom applications. The name of the exchange bears no relation to Canada-based exchange CaVirtex and is not connected in any way.

**Reputational Risk**

- An online boycott campaign is circulating the Internet calling for consumers to boycott a leading U.S. investment bank for charging fees on cashing checks.

- An SEC trial attorney in his retirement goodbye party speech said his bosses were too tentative and fearful to bring many Wall Street leaders to heel after the 2008 credit crisis, echoing the regulator’s outside critics. The attorney, who joined the SEC in 1986, said his superiors were more focused on getting high-paying jobs after their government service than on bringing difficult cases. The attorney states SEC penalties have become “at most a tollbooth on the bankster turnpike.”

- Hackers who recently raided the credit card payment system of a large U.S. retailer belong to a sophisticated Russian syndicate that has stolen more than 160 million credit-card numbers from retailers over seven years. The Russian group is well known to U.S. authorities, who have indicted several members and linked it to pillaging more than 100 companies.

- Russia is urging companies to delist their shares from overseas stock exchanges and trade in Moscow in an effort to safeguard them as international sanctions mount against the country after its takeover of Crimea. Further, the Russian government is creating “attractive” conditions for companies that decide to re-register on OAO Moscow Exchange, and will itself push on with plans to sell state-owned assets on the stock exchange.

- A U.S. District Court judge sided with the Federal Trade Commission’s (FTC) attempt to punish companies for poor security standards that lead to data breaches, as it refused to dismiss the agency’s lawsuit against a hotel and resort chain for getting hacked. The FTC claims the company’s promise to protect users’ data was “unfair and deceptive.”

- The Consumer Financial Protection Bureau recently ordered a leading U.S. investment bank to repay $727 million to consumers wronged by the bank’s deceptive marketing practices regarding credit card add-on products.

A U.S. university law school published a study that concludes minority residents in Minneapolis, MN are “much more likely than white people of similar incomes to be rejected for a mortgage, whether they’re buying a home or refinancing.” The study, using data from 2009 to 2012, focused more on general patterns than on particular bank activity. But it notes the “two largest banks in Minnesota would have made an additional 5,400 mortgage loans in racially diverse and mostly non-white Twin Cities neighborhoods during that period if they had distributed their loans proportionally to the distribution of homeowners with various incomes across the region.”
Global Intelligence

China

- A Chinese news outlet reports the number of NTP DDoS attacks increased and exceeded the number of SYN flood DDoS attacks in February of this year comparing to December, 2013.

- The China Post reported that seventeen independent worker unions in Taiwan released a joint statement, calling on all blue collar workers to protest against the Cross-Strait Trade Services Agreement on May 1, Labor Day.

- The China Labour Bulletin reports on cases of bribery at Ford Motor Company's assembly plant in Chongqing. A recent report by Marketplace reveals that some employees paid their way into the company, not for production or assembly positions but for less labor intensive jobs such as quality control. Ford issued a statement on this matter, saying they have initiated an investigation.

Germany

- The German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt e.V., DLR) in Cologne was apparently targeted in a cyber attack. The DLR involved the German National Cyber-defense Center, a German government agency established to respond to attacks on government computers. The attack is said to show hallmarks of foreign government actors and news reports speculate as to whether Chinese or American agencies are to blame. Multiple computers used by researches and system admins were systematically targeted with spyware.

Israel

- Famed hacking group Anonymous has struck again with attacks on numerous websites operated by Israeli ministries and organizations in an effort labeled as “OpIsrael.” The attacks are in regards to the group’s disagreement with Israeli policies, which include those that affect Palestinian territories. Anonymous introduced “OpIsrael” in November 2012 during an Israeli assault on Gaza. During the initial attacks, some 700 Israeli websites were taken down.

North America

- My Fox Atlanta News reported that Amazon is offering its workers who are not happy to work for Amazon money to quit. The program is called Pay to Quit. After the first year of employment, a worker could get $2,000 in severance pay with the bonus topping out at $5,000 in the fourth year. The theory is that employees who stay, but are unhappy make the work place unhealthy for others.

- Times Union reported that a new agreement with employers gives more than 300,000 tech-sector workers added guarantees that the “always connected” lifestyle enabled by smartphones won't infringe on tech workers' rights under France's 35-hours-work-week. The deal gives workers at risk of burnout a right to disconnect, but does not change their working hours. The deal only covers workers, such as consultants, who already have flexible schedules, not employees on fixed shifts.

- Reuters reported that the NLRB is hearing input from unions, workers, and businesses on the board's proposals to modernize its rules for union elections, which includes allowing electronic signatures and expediting pre-election hearings.

- The SF Gate reported that SEIU filed documents with city's Department of Elections on 4/7/2014 to place a proposal on the November ballot to raise the city's minimum wage
to $15 an hour, the highest in the nation.

- Apple Insider reported that the class action lawsuit from tech sector employees against Silicon Valley tech companies seeks some $9 billion in lost wages. About 100,000 employees are involved in the lawsuit, seeking a payment of about $90,000/person.

- Equity Factor reported that 4/16/2014 SEIU Local 1021 in San Francisco will march to Twitter headquarters and give Twitter a bill for the tax break the company received from the city three years ago.

**Vietnam**

- Lao Dong News reported that workers of MTV Pia Toan Cau had anticipated in getting paid but the president of the company was unexpectedly absent and unreachable. This caused workers to be concerned that they would not get paid. The company owes the workers 1 month, 10 days worth of salary payment. In addition, the company has failed to pay for the workers' health insurance and social insurance for the last 6 months even though the company has been deducting workers' wages for these insurances. The company manufactured clothing and is located in Ho Chi Minh City, approximately 13.4 miles.