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

Top Incidents

**Energy**
- Over the past several months there have been a series of demonstrations at PG&E President Christopher John’s house by Anti-Smart Meter Activists. The group reads their manifesto, shouts out their health issues, posts the manifesto on the door, and leaves a copy of Take Back Your Power (Video on dangers of smart meters),

**Agribusiness**
- A Twitter account representing Anonymous’ OpGreenRights announced on April 18 that it would deface the website of ASA S.p.A., an Italian
"environmental services" company based in Livorno. As of April 21 at 2:00PM EST, the website still displayed an Anonymous logo with a message indicating that the group had defaced the website.

**Insurance/Healthcare**

- According to the results of a recent survey of 595 U.S.-based IT security practitioners, 65 percent of respondents said their companies had experienced SQL injection attacks that successfully evaded their perimeter defenses in the past 12 months. The survey, entitled The SQL Injection Threat Study, was conducted by the Ponemon Institute and sponsored by DB Networks. The survey also found that the average SQL injection breach took almost 140 days to discover and required an additional 68 days to remediate.

**Financial Services**

- An international cybersecurity firm warns while most of the focus on Heartbleed has been on vulnerable public websites, the bug can equally affect client software such as Web clients, email clients, chat clients, FTP clients, mobile applications, VPN clients and software updaters, to name a few. The firm says any client that communicates over SSL/TLS using the vulnerable version of OpenSSL is open to attacks. The bug affects various other servers aside from Web servers, including proxies, media servers, game servers, database servers, chat servers and FTP servers. Finally, hardware devices are not immune to the vulnerability either. The bug can affect routers, PBXes (business phone systems) and likely numerous devices in the Internet of Things.

**Worldwide Intelligence**

- On April 20th, the hacker group NullCrew released an electronic magazine (e-zine) called “FTS Zine 5,” which is a compilation of database information taken from nine different organizations. This has been announced on NullCrew’s Twitter account with details posted to pastebin that includes a link to a compressed RAR file on the website MEGA. The file contains information regarding telecommunication companies, social media sites, gaming servers, as well as state governments. Targets include the University of Virginia, data aggregation website Spokeo.com and recently hacked Klas Telecom.

**Energy**

- Over the past several months there have been a series of demonstrations at PG&E President Christopher John’s house by Anti-Smart Meter Activists. The group reads their manifesto, shouts out their health issues, posts the manifesto on the door, and leaves a copy of Take Back Your Power (Video on dangers of smart meters).

- Speaking before the Senate Energy Committee, Cheryl LaFleur, acting chairwoman of the Federal Energy Regulatory Commission, said they are "wiping and scrubbing all databases." The move immediately follows a government investigator's report revealing unsettling information that certain officials failed to protect the grid's vulnerabilities. They had casually allowed widespread access to a document containing specific physical threats to the grid. The commission has also employed the efforts of a non-profit organization that oversees electric reliability in hopes to improve security standards by June of this year. "A mandatory standard will reinforce these efforts and ensure that all owners and operators of the
bulk power system take such important steps where appropriate," LaFleur said.

- The Nuclear Regulatory Commission has denied a post-Fukushima petition to expand the emergency planning zones around the country's nuclear power plants, saying the current zones are sufficient. The petition was filed in February 2012 by the international nonprofit, Nuclear Information Resource Service, 11 months after the Fukushima Dai-ichi disaster in Japan. It was supported by 37 environmental organizations across the country. More than 3,000 people asked the Nuclear Regulatory Commission to consider them co-petitioners, and nearly 6,000 comments of support were submitted. "The NRC has failed the American people," said Michael Mariotte, president of Nuclear Information Resource Service, in a written statement. "Rather than learn from Fukushima and act appropriately to protect the public, the agency has chosen to protect the nuclear power industry yet again." The petition asked the NRC to expand the current 10-mile-radius emergency planning zone to 25 miles; to create a new, 50-mile "emergency response zone"; and to expand the "ingestion pathway zone" — where drinking water and food could become contaminated — from 50 to 100 miles.

- The Localize This! Great Lakes Basin Action Camp has begun accepting registrations and donations. The event will be held near Kalamazoo, MI, from May 13-20 this year.

- Blue Skies Campaign is soliciting donations for the legal defense of seven activists who were recently arrested for obstructing an energy train in a protest.

- The 10th Annual Mountain Justice Summer Camp will be held on Pine Mountain in Kentucky from June 14 to 22.

- Wild Roots Feral Futures, an activist training camp devoted to ending industrial civilization, has begun crowdfunding this year’s camp, scheduled to take place in Colorado, from June 14 through 22.

- Fugitive jihadist commander Mokhtar Belmokhtar is hiding in Libya, from where he plans to mastermind terrorist attacks across Africa's Sahel region, security sources told Agence France Presse on Sunday. Belmokhtar’s whereabouts were confirmed by a Nigerian security source, and another source close to MINUSMA, the United Nations peacekeeping mission in Mali.

- Researchers from the University of Calgary and Duke University studied property sales from 1994 to 2012 in 36 Pennsylvania counties and seven counties in New York. They mapped sales against the locations of shale-gas wells, and they compared homes connected to public drinking-water systems to homes with private wells. Properties with private wells suffered a loss in value compared to properties connected to a municipal water system, they found, offsetting gains in value from mineral-rights royalties. The loss varied with distance from the nearest shale-gas well. At 1.5 kilometers, properties with private wells sold for about 10 percent less.

- Ohio geologists have found a probable connection between fracking and a sudden burst of mild earthquakes last month in a region that had never experienced a temblor until recently, according to a state report. The quake report, which coincided with the state's announcement of some of the nation’s strictest limits on fracking near faults, marked the strongest link to date between nerve-rattling shakes and hydraulic fracturing.
An analysis of a number of hydraulic fracturing sites in southwestern Pennsylvania has found that methane was being released into the atmosphere at 100 to 1,000 times the rate that the Environmental Protection Agency estimated. The study, published Monday in the Proceedings of the National Academy of Sciences, found that drilling operations at seven well pads emitted 34 grams of methane per second, on average, much higher than the EPA-estimated 0.04 grams to 0.30 grams of methane per second.

The Food & Water Watch Fund has initiated a pledge drive, pushing Pennsylvania candidates to sign the document in which they essentially pledge to “instruct and/or advocate for the Pennsylvania Department of Environmental Protection to cease issuing new hydraulic fracturing well permits until such time as the practice aligns with the people’s “right to clean air, pure water, and to the preservation of the natural, scenic, historic and esthetic values of the environment” as stipulated by the Pennsylvania Constitution. As part of the pledge, if elected, candidates promise to initiate an array of studies focused on determining fracking’s impact on the environment, water quality, climate change, economy, and community.

Greenpeace New Zealand has initiated a campaign titled #SackSimon, in which it seeks to have NZ Energy and Resources Minister Simon Bridges, sacked. Greenpeace accuses Bridges of neglect and carelessness due to his alleged lack of knowledge regarding offshore oil drilling risks, oil spill plans, and conservation park boundaries before issuing off/onshore drilling blocks for lease. The campaign has a petition, which is reached 23,000 signatures, as well as a spoof website, emulating Simon Bridges’ but which appears to be drowning in oil.

Gas extraction produces a range of potentially health-endangering pollutants at nearly every stage of the process, according to a new paper by the California nonprofit Physicians Scientists & Engineers for Healthy Energy, released today in Environmental Health Perspectives, a peer-reviewed journal published by the National Institutes of Health. The study compiled existing, peer-reviewed literature on the health risks of shale gas drilling and found that leaks, poor wastewater management, and air emissions have released harmful chemicals into the air and water around fracking sites nationwide.

New research suggests that pollution from fracking contributes a much larger share of Dallas-Fort Worth’s smog problem than state officials have said. The study, conducted by Mahdi Ahmadi, a graduate student at the University of North Texas, was presented at a clean-air meeting this morning in Arlington. The Observer received a copy of the presentation. Ahmadi analyzed data from 16 air-quality monitors in the Metroplex going back to 1997, looking for a connection between oil and gas production and ozone. Seven of the sites were east of Denton, outside of the Barnett Shale, and nine were located in the shale area, close to oil and gas activity. Ahmadi’s twist is that he adjusted for meteorological conditions, including air temperature, wind speed and sunlight—key ingredients in ozone formation. Backing natural factors out of the data allowed Ahmadi to better pinpoint human factors, including the link between fracking and ozone formation. He found that while smog levels have dropped overall since the late 1990s, ozone levels in fracking areas have been increasing steadily and rising at a much higher rate than in areas without oil and gas activity.
According to the results of a recent survey of 595 U.S.-based IT security practitioners, 65 percent of respondents said their companies had experienced SQL injection attacks that successfully evaded their perimeter defenses in the past 12 months. The survey, entitled The SQL Injection Threat Study, was conducted by the Ponemon Institute and sponsored by DB Networks. The survey also found that the average SQL injection breach took almost 140 days to discover and required an additional 68 days to remediate.

LewisGale Regional Health System of Salem, Va. recently reported a multi-state data breach that affected 400 patients, 40 of which were under LewisGale’s care. The breach occurred in LewisGale’s billing department as a result of a former employee accessing patient data between August 27, 2012 and April 23, 2013. Patient names, addresses, insurance information and Social Security Numbers were all potentially exposed as a result of the breach.

Hackers recently accessed data from approximately 480,000 initial inquiry forms submitted to the U.K.’s Harley Medical Group. The forms included potential clients’ names, addresses, e-mail addresses, phone numbers and birthdates, along with the plastic surgery procedures they were considering.

As different states explore the benefits of big data and healthcare IT analytics, the element of patient privacy is invariably raised as a concern. The technology is in place to make the best use of big data from an organizational standpoint while allowing patients to control their information as well.

Though the Department of Health and Human Services (HHS) released its HIPAA security risk assessment tool a few weeks ago, it’s still unclear how healthcare organizations will use the tool as part of their HIPAA Security Rule compliance strategy.

A new picture-sharing phone and tablet application for doctors and medical students is raising concerns about patient privacy. It allows the sharing of medical and clinical pictures between health practitioners to assist colleagues with patient diagnoses and to aid studying students and is one of three new clinical picture-sharing apps to hit the Australian market this year.

On February 13, 2014, Amerigroup was made aware that an IRS agent and the Tallahassee, Florida, Police department discovered documents containing protected health information (PHI) in screen prints from an Amerigroup claims system while searching the car of a suspect on January 30, 2014. The documents contained the full name, social security number, date of birth, city and state of residence, and Medicare or Medicaid identification numbers and original effective date of 183 Amerigroup Texas Medicaid and Medicare recipients.

Ensuring that privacy and security needs don’t deter from a healthcare organization’s business initiatives, and vice-versa, requires the organization to have a strong understanding of the HIPAA Omnibus rule’s terminology.

Texas’ Lubbock Cardiology Clinic recently published a paid advertisement on the Web site of the Lubbock Avalanche-Journal warning the clinic’s
patients that "an Unauthorized Access into the EHR (electronic health record) containing our medical records" had occurred.

- A recent report released by software vendor IS Decisions, The Insider Threat Security Manifesto, took an international, cross-sector look at the current state of IT security, but there were healthcare information security findings of note as well. According to the results, healthcare suffered double the average amount of internal security breaches compared to the rest of the industries part of the report.

- Tennessee's University Urology recently began notifying 1,144 patients that their names and addresses had been inappropriately provided to a competing healthcare provider.

**Activism**

- Occupy activists held a protest on April 14th in New York City denouncing “wage abuse” by business owners. This is a recurring event that will take place every Monday evening in support of all “wage theft” victims.

- Activists protested against dairy price fixing and global carbon trading at the Chicago Mercantile Exchange (CME) in Chicago, IL on April 18th.

- A ‘Million Mask March’ will occur May 1st at Pershing Square in Los Angeles, CA. The target list includes the Federal Reserve, politicians, leading corporations, and bankers.

- Fossil Free activists are demanding a university in London, UK divest from several financial services institutions, including several leading U.S. banks.

- Multiple activist groups have called to protest at branches of a leading national bank nationwide on April 28th and 29th to denounce their racial discrimination targeting minority communities, investments in the prison and fossil fuel industries and receiving tax rebates.

- Activists will conduct a rally on April 25th in Philadelphia, PA to demand the forgiveness of all student loans and free higher education for all.

- Activists are calling on a leading U.S. financial firm to offer investors a ‘Social Choice’ fund with a low carbon option or move to eliminate any fossil fuel-intensive investments from the current portfolio itself.

- A Michigan-based activist group is calling for a 24-hour occupation of a leading U.S. investment bank branch in downtown Kalamazoo, MI on April 22nd due to the bank’s shares in an energy company that’s believed to be responsible for the July 2010 spill of diluted bitumen into Talmadge Creek near the Kalamazoo River.

- Activists are planning to target multiple banks across New York City from Earth Day (April 22) through May Day (May 1) for their involvement in various initiatives including mountaintop destruction, Keystone XL, coal, foreclosures, and private prisons.

- A delegation of various activist groups traveled to Kansas City, MO April 15th to attend a leading U.S. bank’s annual shareholder’s meeting where
they protested the bank for perceived discriminatory lending practices.

- A Seattle-based housing activist group protested against foreclosures outside a branch of a leading U.S. bank in Seattle, Washington on April 18th.

**Information Security Risk**

- An international cybersecurity firm warns while most of the focus on Heartbleed has been on vulnerable public websites, the bug can equally affect client software such as Web clients, email clients, chat clients, FTP clients, mobile applications, VPN clients and software updaters, to name a few. The firm says any client that communicates over SSL/TLS using the vulnerable version of OpenSSL is open to attacks. The bug affects various other servers aside from Web servers, including proxies, media servers, game servers, database servers, chat servers and FTP servers. Finally, hardware devices are not immune to the vulnerability either. The bug can affect routers, PBXes (business phone systems) and likely numerous devices in the Internet of Things.

- A hacker defaced the website of a local community bank in Colorado while also claiming to have breached its database on April 13th.

- Both Cisco and BlackBerry have found that a variety of their products contain a vulnerable version of OpenSSL. BlackBerry on April 10th said that several of its software products are vulnerable to the OpenSSL bug, but that its phones and devices are not affected. The company said its BBM for iOS and Android, Secure Workspace for iOS and Android and BlackBerry Link for Windows and OS X are all vulnerable to the OpenSSL flaw. Cisco said that many of its products, including its TelePresence Video Communications Server, WebEx Meetings Server, many of its Unified IP phones and several others, are vulnerable.

- An alleged member of Anonymous claims that the Central Bank of Iran's website was adversely affected by cyber-attacks on April 12th.

- The Canadian tax authority announced they have had data stolen by hackers exploiting the Heartbleed bug.

- Microsoft announced this week that it would no longer provide security updates to users running out-of-date versions of Windows 8.1.

- A leading U.S. cybersecurity firm has analyzed the activities of a cybercrime organization that appears to be targeting a wide range of organizations, including financial firms and businesses. The attack starts with a typical spam email that carries an attachment that is a Java archive (.jar). It’s not an exploit but the payload is a multi-platform remote access tool (RAT) called Netwire. In addition, the cybercrime organization is using the DarkComet RAT and the POS malware JackPOS.

- About 2.6 million credit and debit cards were compromised from a breach at a leading U.S. retailer. The breach occurred between May 8, 2013 and January 27, 2014. The retailer disclosed the breach on April 17, 2014.

- A leading U.S. investment firm urged 800,000 customers to change account passwords and other information to protect themselves from risks associated with the Heartbleed computer bug. The bug may have exposed some customers who accessed their accounts on the website for one of the firm’s mutual funds between Dec. 12 and April 14.

- Researchers say cybercriminals have started using a sophisticated Android Trojan app designed for e-banking fraud to target Facebook
users, possibly in an attempt to bypass the two-factor authentication protection on the social network. The new variant of a computer banking Trojan is called Qadars and it can inject rogue JavaScript code into Facebook pages when opened in a browser from an infected system. The injected code generates a message instructing users to download and install Android malware that can steal authentication codes sent to their phones via SMS.

- A new version of an old Java RAT has been detected as JAVA_OZNEB.B and is called UNRECOM (Universal Remote Control Multi-Platform). It was previously known as Adwind. The new RAT is being distributed with the aid of spam emails and often disguised as product lists, catalogues or receipts. The new version also includes Litecoin miner plugin, a cryptocurrency that’s often considered as a popular alternative to Bitcoin. The Litecoin plugin can allow a remote malicious user to use an infected computer to mine Litecoins. Mining digital currencies requires a lot of computing power so victims may experience sluggish performance from their infected computers.

- A leading international cyber-security firm says a banking trojan for Android called Faketoken reached #13 in the Top 20 mobile threats “hit parade”, accounting for 4.5% of all infections. During the first three months of 2014, the firm detected attacks involving Faketoken in 55 countries, including Germany, Sweden, France, Italy, the UK, and the US.

**Legal, Litigation, Regulatory Risk**

- A security researcher notes that under FINRA 7430 for Clock Synchronization, all computer system clocks and mechanical time-stamping devices must be synchronized to any source within one second of the National Institute of Standards and Technology (NIST) standard and updated every business day before market open.

- The SEC unveiled a roadmap on April 15th that lays out how they plan to make sure Wall Street firms are prepared to detect and prevent cyber-security attacks. The document puts firms on alert to be prepared, for instance, to provide a comprehensive list of when they detected malware, suffered a DDoS attack, or discovered a network breach since January 2013. The SEC also plans examinations of more than 50 firms that will focus on cyber security-specific issues.

- A 19-year-old Canadian student became the first person known to be arrested for exploiting the heartbleed bug which left millions of websites vulnerable when it was revealed last week. A resident of London, Ontario, was arrested “without incident” at his home on Tuesday and faces charges relating to stealing the information of 900 Canadian taxpayers from the Canadian Revenue Agency (CRA) website last week.

**Operational Risk**

- Various activist groups will conduct a series of “Earth Day to May Day Direct Action” events that will commence on April 22nd and last through April 30th in Oakland, Berkeley, and San Francisco, California. The events include training days, an Earth Day march (April 22nd); and a critical mass action in San Francisco (April 25th).

- Occupy Wall Street promotes an ‘Earth Day Convergence’ march to occur April 22nd from 5:00pm to 7:00pm EDT that will travel from Zuccotti Park in NYC through the Financial District.

**Reputational Risk**
Multiple activist groups launched an online petition urging supporters to confront Congress and demand that they “stop the corporate tax giveaways.” The petition references multiple financial firms allegedly deploying “schemes” and exploiting “loopholes” to avoid paying any taxes.

An environmental activist group reports progress with its mountaintop removal (MTR) campaign, as a leading U.S. bank updated its environmental policy and divested from a leading MTR offender. The activist group encourages its supporters to use the momentum to send the banks a message and help end MTR coal mining once and for all.

A petition identified at an activist site is directed to the CEO of a leading U.S. bank and calls on the public to sign to “condemn this international bank for lying to customers and cheating them out of their money.”

A coalition of activist groups published a letter on April 14th addressed to 13 financial firms that signed The Green Bond Principals initiative. The letter aims to hold the firms that are currently supporting The Green Bond Principals accountable to the initiative.

· 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 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.”
China

- Chinese news outlets reported over 10,000 workers at shoe-making factories owned by Yue Yuen Industrial in Dongguan took to the streets Monday April 14, 2014, protesting the company's failure to pay its 70,000 employees their full social security and housing fund contributions. Allegedly, the work disruption may affect orders for several top shoe brands such as Nike, Adidas, Reebok, and more. Number of protesters reached 40-60,000 by the end of the week.

Germany

- The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) cautions against a wave of phishing emails with forged information in the header. The headers are manipulated to indicate the BSI itself as sender. The emails threaten legal consequences for alleged violations of certain laws unless an attached form would be downloaded and filled out. The BSI suggests not to open such a message but to delete it and to check any exposed machine with current antivirus software.

- CNet reported that Amazon employees in Germany may be striking again. The German labor union Verdi announced on 4/17/2014 that it has called on Amazon's workers at facilities in Leipzig and Bad Hersfeld to walk off their jobs, arguing that until the Amazon negotiates new wage agreements, employees should not work.

North America

- Times Union reported that Samsung and GlobalFoundries announced an unprecedented agreement to duplicate next-generation chip manufacturing at their factories in South Korea, Austin, Texas, and Malta, NY.

- UniGlobal Union reported that the Global Union Alliance @IBM, alongside UNI Global Union, IndustriALL Global Union and IndustriAll European Trade Union, will issue a series of demands to IBM management designed to protect the firm's loyal workforce.

- The Sacramento Bee reported that about 250 employees of HP's Rosevill campus are being relocated to other locations as part of a restructuring of the company's printing and personal systems divisions.

- WRAL TechWire reported that there is rumor that IBM may announce another round of layoffs.

- The San Francisco Gate reported that several dozen protesters briefly blocked a Google bus on 4/11/2014 near San Francisco's Dolores Park in order to raise awareness about a Google executives they say is evicting multiple tenants from a Mission District apartment.

- The San Francisco Gate reported that San Francisco nurses, janitors, and other workers marched to Twitter's headquarter on 4/15/2014 to deliver a symbolic tax bill for tens of millions of dollars for the "corporate tax giveaway" that helped persuade the company to move to San Francisco's Mid-Market area.

- The Tech Chronicles reported protesters dressed up as Apple Store employees in telltale blue t-shirts marched in front of the Union square store on 4/15/2014 morning, calling on Apple to pay taxes on the $102 billion they said the company holds overseas. SEIU USWW organized the
march.

**United Kingdom**

- On April 20th, the hacker group NullCrew released an electronic magazine (e-zine) called “FTS Zine 5,” which is a compilation of database information taken from nine different organizations. This has been announced on NullCrew’s Twitter account with details posted to pastebin that includes a link to a compressed RAR file on the website MEGA. The file contains information regarding telecommunication companies, social media sites, gaming servers, as well as state governments. Targets include the University of Virginia, data aggregation website Spokeo.com and recently hacked Klas Telecom.

**Vietnam**

- Duong Bo News, a local Vanesa media source, reported that workers from YSVINA, a clothing manufacturing company, went on strike because the company owed workers’ money. In addition, workers complained about having their salary be deducted for unreasonable reasons. Employees cited that they were fined whenever they took time off or when they don’t wear their uniforms.

- Nearly 800 workers from Pia Toan Cau company also went on strike due to the Company's failure to pay workers’ their wages.

- 2000 workers from Wonderful Saigon Electrics, an electronic manufacturing company, went on strike to protest against the company’s change in work schedule. According to the media source, the company change work schedules from 4 days a week to 6 days a week but only increased salary payment by 200,000VND/person.