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

White Paper available:
In this white paper we help you to understand the advanced persistent threats you face, and outline steps to move towards intelligence-led cyber security

Top Incidents

**Energy**

- 28 protesters were arrested at a nuclear reactor in the Netherlands. The protesters attempted to block the entrance of a nuclear power plant prior to the arrival of visiting delegates from the Nuclear Security Summit. The group released the statement, “While politicians in The Hague talk about the reduction of nuclear material and resisting the spread of nuclear technology, in Amsterdam, CEO’s from the most important nuclear power companies have made plans for further spreading the material and the technology.”

**Agribusiness**
A major Spanish news outlet reports that the Live Well Foundation and the Fund for the Defense of Environmental Health has asked top government officials to "reduce the use of pesticides in Spain by 30%".

**Insurance/Healthcare**

- The National Insurance Crime Bureau has released a new report revealing a decline in Florida's personal injury protection (PIP) questionable claims (QCs). In 2013, Florida PIP QCs declined by 7.6 percent from 2012. Meanwhile, for the period 2010 through 2013, Florida staged accident QCs decreased by 61.82 percent.

**Financial Services**

- A hacktivist collective claimed March 24th to have stolen the credentials of over 800 million credit cards, and began a series of posts in the open source leaking multiple files containing data from millions of compromised credit cards. The collective states it will continue to leak credit card credentials, and that the goal for this attack is the downfall of the U.S. economy.

**Worldwide Intelligence**

- The Swiss federal government voted favorably for a revision of a bill on surveillance of electronic communication, which authorizes the use of Trojans for surveillance by government agencies. The Federal Congress will vote on the law, heavily criticized by the Swiss IT sector, in June, while the Pirate Party has announced that it will organize a referendum against it.

**Energy**

- British Columbia newspaper The Vancouver Sun has published a Washington University study on coal train pollution in an effort to bolster opposition to the Fraser Surrey Docks coal export expansion.

- Five Marcellus Shale Earth First! activists were charged in relation to disruptive anti-fracking activities in Pennsylvania last week. All five have since been released on $57,500 bond.

- A recently released and heavily redacted Canadian Security Intelligence Service report shows that the CSIS was monitoring the Idle No More protest movement, and planning in case the movement became violent.

- A new poll shows North Carolina voters across the political spectrum are concerned about future coal ash spills and strongly support new protections to prevent them.

- The new issue of the Earth First! Spring Newsletter features an article about forensic examination of tool marks, with guidelines governing removal of fingerprints from tools, how to change their tool marks between “actions,” and when to discard thee tools.

- A regional summit to organize opposition to the Algonquin Pipeline is scheduled to be held in Voluntown, Connecticut on April 6. Multiple groups from multiple states will be represented.

- 28 protesters were arrested at a nuclear reactor in the Netherlands. The protesters attempted to block the entrance of a nuclear power plant prior to the arrival of visiting delegates from the Nuclear Security Summit. The group released the statement, "While politicians in The Hague talk about the reduction of nuclear material and resisting the spread of nuclear technology, in Amsterdam, CEO’s from the most important nuclear
power companies have made plans for further spreading the material and the technology.

- Scotland’s environmental watchdog has investigated more than 100 incidents involving the wind industry in just six years, including diesel spills, dirty rivers, blocked drains and excessive noise. Warning notices were also issued for the contamination of drinking water and the indiscriminate dumping of waste. Murdo Fraser MSP, convener of Holyrood’s economy, energy and tourism committee, said: “I am both surprised and concerned by the scale of these incidents. “The wind industry constantly portrays itself as being environmentally-friendly and talks about clean, green, energy, but the fact there were more than 100 complaints is a dismal record. “This should serve as a wake-up call that wind energy is not as clean and green as is being suggested.”

- A barge that once carried some 900,000 gallons of heavy tar-like oil was cleared of its remaining contents Sunday, a day after the vessel collided with a ship in the busy Houston Ship Channel and leaked about a fifth of its cargo into the waterway. Coast Guard officials said that up to 168,000 gallons were dumped after one of the barge’s tanks ruptured and that oil had been detected 12 miles offshore in the Gulf of Mexico.

- Hundreds of fracking wells in Pennsylvania have been reported for failures that could lead to air and water pollution, according to a new report. The report, which focused on fracking wells in the U.K. and Pennsylvania, looked at multiple datasets of wells in Pennsylvania to determine their rate of well failures. Researchers found that one-third of a dataset of 3,533 wells in the state had been reported for environmental violation notices between 2008 and 2011. These violations included surface water contamination, land spills, site restoration problems and well barrier failures, including four violations for well blowouts. Another dataset of 8,030 wells contained 506 reports for well barrier failures between 2005 and 2013. The researchers, who are based in the U.K., used this data on Pennsylvania to compare their safety to wells in the United Kingdom. They said there were many unknowns about the safety of fracking wells in the U.K., a finding that pointed to the need for more monitoring and safety precautions for the wells, especially as fracking expands in the country.

**Agribusiness**

- On March 30, the SHAKA movement (closely affiliated with BAB) held a petition-signing event in Maui, seeking to gather the 8,500 signatures required to put a GMO moratorium on the Maui County ballot in 2014. Turnout was considerably higher than expected, and several sources, including Babes Against Biotech and GMO Free USA, claim that “thousands” of protesters were present. The group has not announced whether it acquired the necessary signatures.

- A major Spanish news outlet reports that the Live Well Foundation and the Fund for the Defense of Environmental Health has asked top government officials to “reduce the use of pesticides in Spain by 30%”.

- In a March 25 article a Brazilian agricultural news outlet reports that a federal public prosecutor from Brasilia has asked the Justice ministry to declare a ban on products containing glyphosate.

- Following the declaration by 74 cantons that they had gone “GMO-free” in anticipation of more complete studies on the health effects of GMOs, a major Costa Rican news outlet questions whether the declarations - in most cases, proclaimed independently by each individual canton - hold legal weight.

- Mayans Win Legal Battle to Ban GMO Soy in Mexico’s Campeche Region. Following a
ban on the cultivation of GMO corn in Mexico in 2013, the Campeche region of the country has now prohibited the growing of GMO Soybeans following a two year court battle.

- Brazil’s Federal Appeals Court unanimously decided to cancel the release for cultivation of Bayer’s Liberty Link GMO Corn.
- Syngenta (Canada) halted commercial sales of a new GMO corn strain due to lack of approval for their genetically modified goods. Syngenta’s corn was not approved for sale in Japan, Mexico, South Korea, China nor the European Union.

Insurance

- A September 2013 report by advocacy group Change to Win (CtW) reported that HIPAA-protected patient information, such as medical histories, was left unattended and open to the public in 80 percent of Walgreens stores that are using the “Well Experience” model for their pharmacies.

- The National Insurance Crime Bureau has released a new report revealing a decline in Florida’s personal injury protection (PIP) questionable claims (QCs). In 2013, Florida PIP QCs declined by 7.6 percent from 2012. Meanwhile, for the period 2010 through 2013, Florida staged accident QCs decreased by 61.82 percent.

- During last week’s Health IT Standards Committee (HiTSC) Privacy and Security Workgroup Meeting, members continued to debate and discuss the 2015 notice of proposed rule making (NPRM). Specifically, the group looked at recent draft discussions of EHR authentication, access control, and authorization capabilities.

- Pharmacy fraud has become a rampant problem spreading from Miami across much of Florida, as drug traffickers conspire with doctors and sometimes patients to cheat the Medicare system.

- Matching patients to all the right electronic records and complying with privacy rules that differ from state to state are among the toughest ongoing challenges that health information exchanges face, according to a new Government Accountability Office report.

- Information on 586 children treated at the Arnold Palmer Hospital for Children in Orlando, Fla., may have been exposed when a flash drive was misplaced on January 28, 2014.

- UK HealthCare is notifying 1,079 patients regarding a breach of protected health information. Talyst, a UK HealthCare vendor that provides pharmacy billing management services, reported a password protected laptop was stolen on February 4, 2014. This vendor’s employee had access to protected health information that may have included name, date of birth, medical records number, diagnosis, medications, laboratory results, progress notes, allergies, height and weight, date of service, physician name and clinic. In some cases, name of insurance carrier and insurance identification number may have been on the stolen laptop.

- A Southern California man who ran a durable medical equipment (DME) supply company has been found guilty by a federal jury in Los Angeles for his role in a $1.5 million Medicare fraud scheme and has been convicted of one count of conspiracy to commit health care fraud, six counts of health care fraud, and six counts of aggravated identity theft.

- As a result of a data breach that occurred back in 2010, Stanford Hospital & Clinics and
a former contractor will reportedly have to dole out more than $4 million to settle a class action lawsuit. According to the San Jose Mercury News, 20,000 emergency room patients' data became available in 2010 on a third-party student homework website, which violated California's well-known Confidentiality of Medical Information Act (CMIA).

- Months after the Texas Health Services Authority (THSA) publicized its use of the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF), THSA and the Electronic Healthcare Network Accreditation Commission (EHNAC) announced a public review period for the TX-HIE accreditation program.

- Saint Peter's University Hospital in New Brunswick, New Jersey, has signed a three-year contract with Malta Systems to fully-implement the technology company’s Privasent system. The hospital began a pilot program with the patient identity software in 2013, and has seen success in its patient matching and privacy capabilities.

- Less than half of healthcare organizations participating in the third annual Healthcare Information Security Today Survey say their organization has a documented information security strategy in place. But a sizable majority say their organization conducted a risk assessment in 2013.

- Duke University Health System has agreed to pay $1 million to resolve allegations that it made false claims to federal health care programs.

Financial

Activism

- Three separate environmental activist groups united to conduct an anti-tar sands demonstration on March 20th in downtown Kalamazoo, MI to protest against a leading U.S. oil company. As part of the demonstration, area financial firms invested in this particular oil company were also targeted by protesters calling for the firms to divest from supporting tar sands.

- Housing activists in Seattle, WA conducted their 11th straight weekly protest action outside a leading U.S. investment bank on March 21st, in response to the bank's foreclosure practices against a particular homeowner.

- An international student coalition will launch a 'Reclaim Education' global week of action from May 1st through 8th to protest profit-driven interests affecting education. The week of action coincides with the May Day labor movement to occur May 1st. While no 'Reclaim Education' action details or targets are disclosed, financial firms internationally may be targeted for their perceived role in contributing to rising education costs and student debt.

- A 'Global Bank Run 2014' campaign will occur on May 1st calling for participants to empty their accounts to "show the banks they do not have power over the world anymore, to try to create a better economic system which is not based on fake money, and to spread awareness of the issue with a fractional reserve banking system and the problems that this has caused."

- Multiple activist groups will conduct a rally on April 8th at the UJA-Federation of NY (130 East 59th Street) from 4:00pm to 7:00pm EDT due to concerns regarding the UJA-Federation permitting "extremist anti-Israel organizations to march in the Celebrate Israel Parade on June 1st in New York. These groups encourage Boycotts, Divestment, and Sanctions (BDS) against Israel, seeking to delegitimize and economically weaken the Jewish State."
• Multiple environmental activist groups conducted a fossil fuel divestment rally outside the New York State Comptroller’s Office in New York City on March 27th, stating New York State’s Common Retirement Fund is heavily invested in the fossil fuel industry.

• A U.S. national day of action’ against "spies, lies, and secret files" will occur April 10th with disruptive actions possibly targeting law enforcement and government facilities, and corporations

Information Security Risk

• A group of university researchers published a paper outlining how the Wi-Fi Protected Access 2 (WPA2) protocol can be potentially exposed using de-authentication and brute force attacks. The paper “provides a novel way of successfully exposing WPA2 security issues by using a complete dictionary that generates all the possible printable ASCII characters of all possible lengths.” To prove their point, the researchers analyzed 10 different scenarios, with the main difference between them being the password. In all but one of the cases, the key was easily found, the researchers stated.

• A hacktivist collective claimed March 24th to have stolen the credentials of over 800 million credit cards, and began a series of posts in the open source leaking multiple files containing data from millions of compromised credit cards. The collective states it will continue to leak credit card credentials, and that the goal for this attack is the downfall of the U.S. economy.

• Cyber thieves stole approximately 1.55 million in a digital currency called BlackCoin, worth 120 Bitcoin, or about $70,000, from exchange site Cryptorush. Reportedly thieves took advantage of a glitch that allowed users’ balances at the exchange to be inflated to an extra 22 million coins, allowing them to withdraw more than they had.

• A research firm published a March 25th report on underground markets for cyber-crime tools which concludes that stolen Twitter accounts now fetch more than credit cards on the cybercrime black market because Twitter account credentials potentially have a greater yield for both the access the account provides to a user's other accounts, and the increased value of a “real” account for spammers. The report says the overall change in social media account value is part of a larger trend in the evolution of the black market for hacks, cracks and data.

• A security firm issued a report that analyzed almost a quarter of a million DDoS attacks in Tier-1 and Tier-2 data centers operated by ISPs and major companies throughout 2013. The company says that DDoS attacks are now frequently being used to hide APT attacks and that DDoS amplifications attacks are also on the rise and are continuing to be a challenge for all business internet users, due to the volume of data generated.

• A security firm discovered that hackers are compromising online banking and social media users in a man-in-the-middle attack campaign that involves posing as major organizations, without setting off alerts. PhishLab observed spam emails containing an RTF file, named ‘Authorization Form’ or something similar, that are actually backdoor Remote Administration Tools (RAT) that surreptitiously execute upon being clicked. The malware reconfigures the DNS settings on the infected PC so that it uses the DNS server controlled by the hacker.

• A researcher discovered a WinRAR vulnerability, a popular software that essentially compresses and decompresses ZIP files, in a malware campaign that seems to be targeting government and international organizations, as well as Fortune Global 500 companies. The vulnerability allows an individual to create a ZIP file that appears to contain one thing when compressed, but actually houses something different altogether. From an attacker's standpoint, they can effectively compress a trojan, or some other malware, with WinRAR and make it seem like the created ZIP file contains an image, or something else that appears harmless. The attacker then waits for someone to click on
the file, which is actually an executable, and the target is compromised.

**Legal, Litigation, Regulatory Risk**

- South Korea announced March 24th it has opened a gold trading exchange for the first time in a bid to help counter the country's burgeoning black market activities surrounding the precious metal. The Financial Services Commission noted it has resolved to intensify a crackdown on black market transactions, with smuggled gold being traded secretly through underground structures as an effective way of hiding income and avoiding tax.

- The U.S. enforced its first convictions on two Florida men for illegally distributing counterfeit mobile apps, after the men pleaded guilty for their part in a scheme that sold pirated apps with a total retail value of more than $700,000. Both men were in the Appbucket group which made and sold more than a million copyrighted Android mobile apps through the group's alternative online market.

- The U.S. SEC announced it will examine the exposure of stock exchanges, brokerages and other Wall Street firms to cyber-attacks that have been called a threat to financial stability. The agency also will probe how public companies are disclosing cyber threats in filings provided to investors. More than half of the exchanges surveyed globally in 2012 said they experienced a cyber-attack, while 67 percent of U.S. exchanges stating that hackers tried to penetrate their systems.

- The head of the European Union's policing agency warned March 24th that virtual currencies such as Bitcoin were being used for money laundering and called for police to be given more powers to identify criminal suspects operating on the Internet. Europol has no policing powers of its own, but acts to coordinate policing and cross-border investigations between the 28 member countries of the European Union. The EU policing agency head said police do not have sufficient capabilities to operate online and identify anonymous groups that are using dark areas of the internet.

**Operational Risk**

- Activists organized weekly conference calls from March 25th to July 8, 2014 to help organize and plan Wave of Action events. Wave of Action is an Anonymous and Occupy Wall Street affiliated campaign that calls for supporters to unite and take action against any type of perceived corruption. Phase I of the Wave of Action campaign will begin April 4th in New York City.

- Occupy members are creating a jail support system for activists arrested during Wave of Action disruptions in NYC on April 4th. The system will track, wait for, and then greet those arrested as they are released from the NYPD Central Booking Station with the likely intent to inject activists back into Wave of Action disruptions.

- Occupy members are creating a "report backs" system to utilize during May Day actions in NYC (May 1) in which activists will report back to Liberty Plaza with possible updates or intelligence as a means to adjust and improve effective disruptive actions throughout NYC.

- Occupy activists created a new initiative that aims to provide alternatives to the centralized banking system that keeps too-big-to-fail banks from failing, noting “the Federal Reserve is owned by Wall Street, not the Federal Government.” The initiative is the first step activists are “concocting to occupy Wall Street, the Federal Reserve and the United States Congress.” Further, activists will conduct an informative presentation on April 4th at the NYC Federal Reserve from 8:00pm to 11:00pm EDT as a "contribution to the World Wide Wave of Action kick-off party."

- An online petition is circulating that calls for U.S. banks to stop charging ATM fees to welfare recipients.
Occupy activists are organizing multiple protest marches to occur along Wall Street in New York City on April 4th as part of the Worldwide Wave of Action campaign.

**Reputational Risk**

- The Federal Reserve Bank of New York issued a report which details why "too-big-to-fail" banks are bad for the economy, noting these banks benefit from significant discounts on bond issues due to an assumption on the part of investors of government bailout protection.

**Global Intelligence**

**Brazil**

- The Brazilian Chamber of Deputies, one of two chambers of the Brazilian legislature, passed the Marco Civil da Internet, a symbolic bill which determines the “rights and duties” of Brazilian internet users. The bill guarantees the principles of net neutrality and forbids the “violation of user data”. More controversial aspects of the bill – including a requirement that all user information be stored on Brazilian servers – were removed. The bill has now been submitted to the Senate.

**Costa Rica**

- Hundreds of public employees staged several protests across Costa Rica on March 20, against a 0.43 percent government-backed wage hike, which demonstrators said was too little to meet basic costs. The demonstrators also protested against the granting of public works concessions to international companies, the privatization of public services, low wage increases and recent hikes in public services rates. The nationwide strike was organized by public-sector unions and included employees from the Social Security System (Caja), the Education Ministry and Caribbean dock workers.

**Germany**

- Starting March 31, 2014, the four leading German email providers (T-mobile, Freenet, Web.de, and GMX.de) are encrypting all email traffic. This is part of the initiative “E-Mail made in Germany”, which provides for transport encryption (but not necessarily end-to-end encryption) and a commitment to store all data in data centers physically located in Germany.

**India**

- IBN Live reported that employees at the India Nokia plant in Sriperumbudur will go on a one-day hunger strike on 3/31/2014.

**Japan**

- Japan Times reported that Toyota will resume "limited production" after unionized employees at its Indian plant refused to return to work following an end to a company lockout. The workers and the company’s management at two plants near the high-tech city of Bangalore are at loggerheads over pay issues, which they have been negotiating for 10 months. Intel has several locations in Bangalore, India. The strike took place at the Toyota plants near Bangalore, India.

- On March 31, The International Court of Justice in The Hague ruled that it did not recognize Japan’s whaling activities as “scientific” and ordered the country to cease those activities. The move puts the future of Japan’s whaling program in question and will likely draw strong opposition, as the mayor of Shimonoseki has already spoken out
in support of the program.

**North America**

- The Examiner reported that a poll of 500 likely voters in San Francisco found 79% of participants believed tech’s growth has been good for the city. Overall, the poll showed that 57% of the people surveyed had a favorable view of the shuttles, 67% disagreed that commuter shuttles are ruining the character of San Francisco.

- NDTV Gadgets reported that Facebook was one of the biggest Silicon Valley companies to have resisted rivals' entreaties to stop poaching each other's employees. The article mentioned Intel agreed to avoid soliciting employees from other tech companies.

- TechWire reported that Lenovo has reaffirmed its commitment to hire some 2,000 IBMers in RTP. The proposed IBM-Lenovo deal received government approval in India, but government regulators elsewhere, including the US, still have to sign off on the $2.3 billion sale.

**Spain**

- A Spanish media outlet reported that this spring Intel will close its research center in Barcelona, located in the Nord de la Universitat Politècnica (UPC). This week Intel is expected to present a notification of termination (ERE) that will affect about seventy workers, most of them highly skilled software engineers. The media also noted that Intel may keep some of the employees if they agree to move to a research center in another country. The closure of the facility is part of the company’s decision to reduce 5% of its workforce due financial results below expectations.

**Switzerland**

- The Swiss federal government voted favorably for a revision of a bill on surveillance of electronic communication, which authorizes the use of Trojans for surveillance by government agencies. The Federal Congress will vote on the law, heavily criticized by the Swiss IT sector, in June, while the Pirate Party has announced that it will organize a referendum against it.

**Vietnam**

- Info.VN reported that Vietnam's CPI in March decreased by .44% against the previous month due to declining demand for goods and services after the Lunar New Year festival.