Welcome to the Cyveillance Weekly Trends Report

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

In this Issue:

- Top Weekly Incidents
- Energy
- Agribusiness
- Insurance / Healthcare
- Financial Services
- Global Intelligence
- Legal and Regulations

New Whitepaper: The 2014 World Cup in Brazil: Examining Physical and Cyber Threats

From June 12 to July 13, Brazil will host the 2014 World Cup soccer competition. Learn more about the potential physical and cyber threats from terrorist and insurgent groups, disruptions from national and international activists, the impact of social media, and other security issues that may impact this event.

Click Here To Learn More

Top Incidents
Energy

- A makeshift bomb exploded at a Nogales, Ariz., power plant Wednesday morning, damaging a large fuel tank and prompting an investigation by the FBI and federal bomb experts. Local officials were alerted at 9:30 a.m. to "suspicious activity" at UniSource Energy Services' Valencia Plant. The explosion damaged a diesel storage tank, but there were no reports of injuries and authorities said they knew of no suspects or witnesses.

Agribusiness

- ABC News published a story about the current national GMO labeling debate. If current bills being considered in New York are passed, existing GMO labeling legislation in Connecticut would go into effect. Additionally, the article mentions the influential power that New York would have as a model for over two dozen other states where GMO labeling legislation has been introduced. This story has been posted on social media by various groups, including one example included in the supplemental section of the report.

Insurance/Healthcare

- District Attorney Jackie Lacey says insurance fraud is on the rise in California, which ranked first in the number of questionable claims in 2012.

Financial Services

- A leading cyber security firm claimed dozens of cybercrime groups have reached the level of sophistication where their technical capabilities are on a par with those of a nation-state. These criminal organizations are capable of building complex systems aimed at stealing money and intellectual property on a grand scale, costing almost the same to the global economy as counterfeiting or the narcotics trade — more than $400bn a year.

Global Intelligence

- Amidst the 2014 World Cup in Brazil, Anonymous defaced several Brazilian government websites and hacked into the Brazilian Foreign Ministry's server, compromising emails and attachments. On June 11, 2014, Anonymous also took credit for other site-crashes that have since been repaired. A couple of sites include the Brazilian Intelligence System and the Brazilian Football Confederation. Anonymous has stated that it is "pursuing the government of Brazil because of their corruption and actions against the people."

Legal and Regulations

- The Department of Justice continues to aggressively pursue its enforcement agenda when it comes to ensuring that websites are accessible to persons with disabilities under the Americans with Disabilities Act ("ADA"). Last week, the DOJ settled its first enforcement action requiring the settling party to make its mobile app ADA-compliant. The settlement is the first of its kind, considering that the DOJ has yet to issue proposed regulations defining the standard for what constitutes an “accessible” website. If you operate a retail website or mobile app, you should pay close attention to these developments and ensure that your site and app are in compliance.
• BoldNebraska.org discusses how Native American groups intend to meet President Obama on his visit to “indian country” with anti-Keystone XL signs and slogans.

• ThinkProgress.org posts an article discussing a new report published by the Center for Biological Diversity and three other health and environmental groups, which found that the oil and gas industry in the Los Angeles area used about 22,500 tons of chemicals that, if released into the air, can be toxic and even carcinogenic last year. According to the report, more than half of these fracking, acidizing, and gravel packing events occurred within 1,500 feet of a school, home or medical facility, with some occurring as close as 12 feet away from these buildings. The report highlights acidizing done by one oil and gas company that occurred 85 feet from houses, 145 feet from a church, and 770 feet from an elementary school.

• TheHill.com reports that a group of states led by Ohio is working with energy companies, government agencies and universities to research how regulations on hydraulic fracturing, or fracking, could prevent human-caused earthquakes. The effort comes after Ohio officials concluded that five small earthquakes in eastern Ohio were probably caused by fracking and injecting fracking waste into the ground.

• ThinkProgress.org reports that U.S. District Judge Kristine Baker denied ExxonMobil’s motion to dismiss a lawsuit claiming the company violated federal and state clean water laws when its Pegasus Pipeline ruptured in March 2013. The judge said the lawsuit offered sufficient proof that ExxonMobil may have committed two violations of the Clean Water Act, two violations of Arkansas’ air and water regulations, and one hazardous materials violation.

• EcoWatch reports that More than 100 people held a demonstration in Bonn, Germany outside the venue where the ministers of environment are meeting for the United Nations (UN) climate negotiations. Organizations from every continent—including trade unions, social movements, environmental groups, gender and youth groups, indigenous groups and NGOs—are demanding action by the more than 198 member governments of the UN Framework Convention on Climate Change (UNFCCC).

• The Indian government says opposition from several nongovernmental organizations, including Greenpeace, to development projects like nuclear and coal plants in the country will cut economic growth by 2-3 percent per year. A report from India’s Intelligence Bureau, dated June 3 and entitled “Impact of NGOs on Development,” claims the organizations and their international donors are planning to protest many budding economic development projects. The report lists seven projects and claims they were each stalled because NGOs led agitation against nuclear power plants, uranium mines, coal-fired power plants, farm biotechnology, mega industrial projects, hydroelectric plants and extractive industries. Intelligence Bureau Joint Director S. A. Rizvi accuses Greenpeace, the largest international NGO listed, of breaking laws to “change the dynamics of India’s energy mix,” using its “superior network” of Indian organizations to stir anti-nuclear agitations and mount “massive efforts to take down India’s coal-fired power plants and coal mining activity.”

• A makeshift bomb exploded at a Nogales, Ariz., power plant Wednesday morning, damaging a large fuel tank and prompting an investigation by the FBI and federal bomb experts. Local officials were alerted at 9:30 a.m. to “suspicious activity” at UniSource Energy Services’ Valencia Plant. The explosion damaged a diesel storage tank, but there were no reports of injuries and authorities said they knew of no suspects or witnesses. Wednesday evening, agents were still processing the scene. Arizona Corporation Commission spokeswoman Rebecca Wilder said there were no power disruptions and the plant received only minor damage. “The reason for the high-scale response is the plant is an electrical substation and critical to the area,” Nogales police Lt. Carlos Jimenez said, explaining that as many as 30,000 customers depend on the plant for power. “The whole city of Nogales could have been compromised,” he added. Authorities described the explosive as “a suspicious device” but would not elaborate.
• A group of activists in Spokane, WA arranged a 40-person energy train protest with only 12 hours’ notice. The protest was prompted by news of a visit by the Governor, and demonstrates the highly connected, committed and organized nature of activists in the region.

• Butte County, CA fracktivists are crowdfunding efforts to push a ballot initiative fracking ban.

• The Greenpeace ship Rainbow Warrior is in Ibiza, Spain in order to help organize opposition to offshore oil drilling plans in the region.

• The Greenpeace Esperanza is targeting ExxonMobil’s semi-submersible rig West Alpha in the Norwegian fjord in Olen near Haugesund.

• Colorado activist group Clean Water Fund has launched a “failure to lead” campaign against Governor Hickenlooper.

---

**Agribusiness**

• ABC News published a story about the current national GMO labeling debate. If current bills being considered in New York are passed, existing GMO labeling legislation in Connecticut would go into effect. Additionally, the article mentions the influential power that New York would have as a model for over two dozen other states where GMO labeling legislation has been introduced. This story has been posted on social media by various groups, including one example included in the supplemental section of the report.

• Article from Burlingtonfreepress.com published June 13, 2014 details the suit officially filed on Thursday June 12 against the Vermont state GMO labeling bill. This story has been circulated on many other media sources and social media, on example of which is included in the supplemental section of the report.

• Article by WNPR questions whether Vermont will be able to defend its GMO labeling law against the Grocery Manufacturers Association, and argues that the state of Vermont is unprepared to fund an ongoing lawsuit, citing the state’s implementation of a donation campaign as evidence that it has not prepared fiscally for the anticipated lawsuit.

• Sustainable Pulse reports that Kyrgyzstan has passed a ban on the cultivation, import, and sale of all GM crops, and that the bill is currently waiting for the President’s signature.

• Reports have been published about the impending reforms resulting from the military coup in Thailand on May 22. The military government has unveiled plans to implement farming reforms moving towards organic farming to benefit farmers and avoid the need to buy expensive pesticides.

---

**Insurance**

• Canada’s Rouge Valley Centenary Hospital recently acknowledged that two former hospital employees had leaked as many as 8,300 patients’ personal information to outside companies.

• The Connecticut state health insurance exchange, Access Health CT, is handling a patient a data breach that occurred when its vendor Maximus’s employee lost a
backpack containing 413 patients' information in a deli.

- Walgreens recently began notifying an undisclosed number of customers that their personal information may have been stolen by a former pharmacy employee in Atlanta, Ga., between March 3, 2014, and April 14, 2014, and provided to a third party.

- Penn State Milton S. Hershey Medical Center began alerting 1,801 patients last week that an employee had accessed clinical data without having proper IT security protections in place.

- A council leaked personal details of housing benefit claimants, including their dates of birth and national insurance details, in response to a Freedom of Information (FOI) request. Basingstoke and Deane sent letters of apology to 1,900 people, warning them their details had been disclosed.

- The personal details of 1,000 patients have been accidentally released by a hospital trust to two research companies, it has been revealed The data breach by Heatherwood and Wexham Park Hospitals included patient NHS numbers and ethnicity details.

- Role-based access control management, which limits the access that users have to data based on their job responsibilities, can be important in efforts to prevent data breaches and safeguard patient privacy.

- A thumb drive containing health records of nearly 34,000 patients was stolen from a Santa Rosa medical office last week. The drive was stolen June 2 from an unlocked employee locker at the former Redwood Regional Medical Group imaging center.

- The Apple HealthKit will serve as a single user interface for the various healthcare applications that the user downloaded, which will be connected to electronic health records (EHRs).

- Health insurer Highmark recently began notifying 3,675 of its Medicare Advantage members that their personal and medical information may have been disclosed to others by a mistake in the mailroom.

- District Attorney Jackie Lacey says insurance fraud is on the rise in California, which ranked first in the number of questionable claims in 2012.

- Today, to share sensitive mental health information, behavioral health professionals largely depend on getting patient consent and then sending confidential paper records to the patient's other clinicians, with strict rules about re-disclosure. But privacy and security experts envision a day when that data can be securely transmitted electronically.

Financial

- **Activism**

  - Labor activists conducted a minimum wage rally on June 10th at the Rhode Island State House in Providence, RI, accusing Rhode Island political leadership of adding a “last minute” bill to the state’s 2015 budget that rejects raising the minimum wage.

  - Labor activists in NYC conducted a rally on June 15th in Herald Square, demanding a minimum wage increase to $15 per hour.

  - Housing activists in Minnesota will conduct a street action on June 17th in Minneapolis to bring attention to an activist group’s national report on the United States’ ongoing housing crisis.
• Activists in England will conduct an anti-austerity demonstration in London on June 21st.

• Housing activists called on their supporters to email Congress to demand Congress vote ‘no’ on a proposal that bans the Federal Housing Administration from backing any mortgages that were refinanced via the eminent domain process.

• Housing activists conducted an anti-foreclosure protest in Los Angeles, CA on June 11th.

• Housing activists held a protest on June 12th in Los Angeles, CA demanding better housing policies.

• Housing activists held a protest on June 12th in Decatur, GA demanding better housing policies.

• Housing activists will “pack the courtroom” on McDonough Street in Decatur, GA on June 16th for the hearing of local residents who were evicted from their homes.

• Housing activists in Dorchester, MA occupied a vacant home owned by a government-sponsored mortgage association as a symbolic step toward reclaiming a neighborhood “plagued” by rising housing costs that have led to foreclosures and evictions.

• Housing activists continued to protest outside a foreclosed home in Dorchester, MA on June 10th, calling for more affordable housing in the Boston area.

• Housing activists held a protest on June 14th in Santé Fe, New Mexico, demanding better housing policies.

• Housing activists held a protest on June 14th in San Francisco, CA demanding better housing policies.

• Housing activists will hold a protest on June 19th in San Francisco, CA demanding better housing policies.

• Housing activists will hold a protest on June 28th in New York City for “Housing Justice.”

• Activists launched a petition to expose a leading U.S. bank after a whistleblower leaked alleged undisclosed secrets from the bank.

• Activists marched to a local office of a government-sponsored mortgage association in Pasadena, CA, demanding the company allow foreclosed homes to be repurchased by their previous owners.

**Information Security RisK**

• A leading security research firm released a threat advisory outlining new payloads from the Zeus toolkit that it has seen in the wild. In addition to the data theft and financial fraud Zeus is known for, researchers discovered Zeus being used in crypto-currency mining, spam, distributed denial-of-service (DDoS) attacks, and attacks customized for specific PaaS and SaaS infrastructure.

• Researchers found a new commercial Trojan malware application called ‘Pandemiya’ that has recently been promoted in underground forums as an alternative to more widely used Zeus Trojan and its variants. The new malware is designed to enable a botmaster to spy on an infected computer – secretly stealing form data, login credentials and files from the victim, as well as taking snapshots of the victim’s computer screen. This malware also allows the injection of fake pages into an internet browser in an effort to gather additional sensitive information from the victims themselves. Pandemiya also includes protective measures to encrypt the communication with the control panel, and prevent detection by automated network analyzers.
A hacker claimed he can use open source software and hardware to replicate NSA's ANT spy tool which was leaked by Edward Snowden. The engineer claims his replicated NSA spy tool can be used to monitor and locate mobile phones, tap USB and Ethernet connections, maintain persistent malware on PCs, communicate with malware across air gaps, and more.

A leading cyber security firm claimed dozens of cybercrime groups have reached the level of sophistication where their technical capabilities are on a par with those of a nation-state. These criminal organizations are capable of building complex systems aimed at stealing money and intellectual property on a grand scale, costing almost the same to the global economy as counterfeiting or the narcotics trade — more than $400bn a year.

The central bank of England released a new cybersecurity framework designed to help financial institutions in the country identify areas of vulnerability that could be exploited by a cyber-attack.

Researchers discovered a new Zeus variant called "Maple" that has targeted 14 leading financial institutions in Canada with the malware since January. Among Maple's enhanced features are "re-patching" techniques, which restore web-injection functionalities (for stealing financial data from web browser sessions) even after security solutions detect the malware. In addition, the Maple variant was designed with anti-debugging features — using a packer written in Visual Basic, a programming language "notoriously complex to debug [that] makes the analysis more difficult.

Researchers said the BKDR_VAWTRAK banking malware identified in Japan is using Windows Software Restriction Policies (SRP) to restrict the privileges of security software.

A hacker claimed to have taken down the official website of a leading Brazilian bank.

Researchers said an Android Trojan program called 'Svpeng' that was originally designed to steal mobile banking credentials from Russian users, was recently retrofitted with ransomware functionality and has started infecting users in the U.S.

A national restaurant chain confirmed that it's looking into a payments breach that may have exposed credit and debit cards used at its restaurants. The company said it's working with authorities to learn more about the nature of the apparent breach and subsequent fraud that has been reported at several of its locations nationwide.

An investment firm in Wellesley, MA reported they suffered a data breach in early April of 2014 due to a malware infection, exposing the personal information of some of their clients.

Researchers said attackers may have infected nearly 350,000 systems with ransomware and earned more than $70,000 in Bitcoins as part of an ongoing phishing scheme leveraging a well-known file hosting service.

Two 14-year-old Canadian schoolboys hacked an ATM of a leading Canadian bank after finding an operator's manual online. The manual showed how to gain administrative control of the device.

**Legal, Litigation, Regulatory Risk**

- SEC Chair Mary Jo White said the agency will consider if revisions are needed to Regulation NMS. White mentioned that the Commission “will be considering whether the SEC’s own rules, such as the trade-through rule of Regulation NMS, have contributed to excessive fragmentation across all types of venues.”

- A class-action complaint alleged U.S. stock exchanges provided market data earlier to high-frequency traders while sending other investors “stale” information. The suit was
filed in May in the Southern District of New York.

**Operational Risk**


**Reputational Risk**

- Activists accused a leading U.S. bank of co-sponsoring an American Islamic banquet event that was held back in March in Chicago despite a federal court's verdict that the organization is linked to the terrorist group Hamas.

- An activist group claimed a leading U.S. bank might be fined $12 billion for its misconduct during the 2008 financial crisis, calling it a "cover up" by the government for "trillions" in losses caused by many national banks.

- A financial media outlet published a report on the 10 highest paid CEOs in the U.S. Banking Industry for year 2013, noting the median compensation total for CEOs at 617 banks rose by 48% from 2009.

**Global Intelligence**

**Brazil**

- Amidst the 2014 World Cup in Brazil, Anonymous defaced several Brazilian government websites and hacked into the Brazilian Foreign Ministry's server, compromising emails and attachments. On June 11, 2014, Anonymous also took credit for other site-crashes that have since been repaired. A couple of sites include the Brazilian Intelligence System and the Brazilian Football Confederation. Anonymous has stated that it is "pursuing the government of Brazil because of their corruption and actions against the people."

**China**

- A Chinese news outlet reported that an arbitration committee in Xiamen, Fujian recently ruled on a series of compensation-related worker strikes, and determined for the first time that the company in question illegally terminated labor contracts before relocating. This indicates that the worker strike was not illegal. Furthermore, the company (Xiamen Delta Tech Controls Electronics) has been ordered to provide appropriate monetary assistance to the workers.

- The Wall Street Journal reported on the increasing labor activism by disenfranchised workers in China, as demands for expanded social and economic rights continue to grow. The article highlights a recent report published by Hong Kong-based rights group, China Labor Bulletin (CLB), in which findings show workers to be a strong, active, collective force in labor dispute negotiations.

- Yahoo! News reported that China issued a statement on 6/8/2014 in defense of its use of an oil rig in contested waters that is at the center of a bitter dispute with Vietnam. It accused Vietnam of acting aggressively towards Chinese personnel, accusing VNese vessels of "illegally and forcefully disrupting" work there and ramming Chinese boats. On 6/8/2014 Vietnam released dramatic footage showing a large Chinese ship chasing and ramming one of its fishing boats which then sank near the rig.
- A Chinese news outlet reports due to World Cup approaching, lots of mobile device betting applications infected with trojan are flooding the market.

- A Chinese website reports a security vulnerability on QQ Group (QQ Qun). According to the article, the attacker could exploit the vulnerability by sending a specific URL within the group, a malicious Javascript source code will be triggered when users check the group message and will allowed the attacker to steal personal information.

**Germany**

- The German Federal Ministry of the Interior establishes two new administrative groups, “IT and Cyber Defense, Secure Information Technology” and “Cyber Security Regarding Police and Domestic Intelligence Service” in order to address cyber threats aimed at German security authorities and public infrastructure. It is pointed out that this is not just a reorganization effort, but the build-up of new resources and that it would reflect the central policy decisions of the administration.

**Korea**

- The Hankyoreh, a Korean media source, reported that the director-general of the International Labour Organization (ILO) suggested an inspection team may be sent to South Korea to examine the labor rights situation.

**North America**

- The Huffington Post reported that the Federal government is offering incentives to lure tech talent away from Silicon. The article reported that the nation's capital is sharing its work on GitHub to appeal to coders and opening up office in San Francisco for those who don't want to live in Washington.

- Chron reported that HP has confirmed that it's layoff plans have extended from the end of October 2014 with 27,000 cuts to May 2015 with the total of 45,000 to 50,000 cuts.

- Triple Trempo reported that after 3 years of controversy Apple, Google, Intel and Adobe have agreed to pay $324.5 million in order to settle the lawsuit filed against them by 64,000 employees. According to the article, the agreed settlement, however, is only a pittance of the potential damages sought. It will only give each of the 64,000 employees a few thousand dollars.

- Times Union reported that Cisco plans to expand its third-largest site by adding 550 jobs at its Research Triangle Park hub before 2018. Cisco plans to hire finance, operations and advance network services workers at an average salary of nearly $73,000/year.

**Malaysia**

- A Malaysian news outlet reports the opposition political group, People Alliance urges the government to raise minimum wage to RM1,100 in order to be higher than poverty line.

**Vietnam**

- ChaoBuoiSang.Net, a local VNese media source, reported that China's government has issued a decision that temporarily prohibits its state-owned businesses from joining projects in Vietnam. According to the article, this is a sign showing that China is attempting to play the economy card.

- VN Review, a local VNese media source, reported that many foreign investors like Intel, Samsung, Canon, Fujitsu... are leaning towards transferring their factories to Vietnam. That is why the regions need to develop the appropriate plans to "catch the wave." The article cited that Intel intends to transfer it's factory from Costa Rica to Vietnam. The article mentioned that Samsung has plans to transfer some of its factories from China over, Canon, Fujitsu also have similar leanings.
• Lao Dong News reported that the current minimum wage is only able to cover 70% workers’ minimum living standards. According to the article, many workers have to work 12-14 hours/day to make enough to cover their living expenditures.

• Truong Tan Sang, a local VNese media source, reported that Samsung is currently contemplating investing over 1 billion dollars into a 3rd factory in Vietnam. According to a senior official at Vietnam’s Ministry of Planning and Development the agency is currently reviewing Samsung’s proposal before granting licensing. Samsung’s representative stated that it is planning to invest in another factory but did not provide more information. If confirmed, this would be Samsung's 3rd factory in Vietnam. Samsung built a factory in Vietnam in 2009 and 2013 worth $2.5 billion and $2 billion respectively.

Legal and Regulations

• Financial Accounting Standards Board release new rules about revenue recognition. While the new standard does not become effective until December 15, 2016 (so it will be applied by calendar-year companies for their 2017 reporting years), companies are being urged to begin thinking soon about implementation. For example, companies will need to assess “whether they currently capture the information they will need to comply with the new standard, both the accounting and the disclosures, and determine if new systems will be necessary. According to this article in Compliance Week, the new rules may result in “dramatic changes that could affect accounting processes in as little as six months.” Commentators observed that the new standard will also “have implications for the sales process, information systems, internal controls, taxes, debt covenants, and potentially even compensation….”

• A recent decision from the National Labor Relation Board’s (“NLRB’s”) Division of Judges further exemplifies the NLRB’s proactive approach in scrutinizing both union and non-union employers’ social media policies. In Kroger Co. v. Granger, the judge found that several provisions of the supermarket chain’s social media policy violated the National Labor Relations Act (“NLRA”). If an employer has a social media policy, it likely contains some provisions similar to the overbroad ones in this case. Below are the top takeaways for employers:

  1. Carefully tailor required disclaimers that employees do not speak for the company.
  2. Be cautious about requiring company permission to use intellectual property — including logos or banners.
  3. Avoid overbroad restrictions on discussing confidential or proprietary information.
  4. Do not prohibit online behavior that reflects negatively upon the company.

• Kroger was ordered to post notices stating that the company had violated federal law, to immediately cease enforcing the policies, and to amend or rescind them within 14 days.

• The Department of Justice continues to aggressively pursue its enforcement agenda when it comes to ensuring that websites are accessible to persons with disabilities under the Americans with Disabilities Act (“ADA”). Last week, the DOJ settled its first enforcement action requiring the settling party to make its mobile app ADA-compliant. The settlement is the first of its kind, considering that the DOJ has yet to issue proposed regulations defining the standard for what constitutes an “accessible” website. If you operate a retail website or mobile app, you should pay close attention to these developments and ensure that your site and app are in compliance.
Financial

- The Treasury Department has posted the first searchable list of about 77,000 foreign financial institutions (FFIs) around the world that have registered to comply with the Foreign Account Tax Compliance Act, including some large U.S.-based banks with foreign operations. The list includes financial institutions and branches with an approved status as of May 23, 2014.