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**

Social Media Watch: Cyveillance now offers services designed to help smaller organizations, particularly banks and credit unions, monitor social media for risk and compliance. Cyveillance Social Media Watch leverages the same proprietary platform, reporting capabilities, and in-depth analysis that power solutions for Fortune 500 customers, but is scoped to address the budgets, needs, and risks of smaller companies. Service elements include Monitoring, Vetted Alerting, Incident Investigation Reports, and Global Intelligence.

Top Incidents

**Energy**

- Activists will be holding the 2nd annual Hands Across the Sand event on May 17. This is a National Day of Action held in beach locations on multiple continents in order to protest pipeline, export and offshore energy projects.

**Agribusiness**

- Due to recent crackdowns from the Chinese government, it is forecast that palm oil
imports from the world's #2 importer will fall. Palm oil had been a commodity that was commonly used for financing in China, but the government has tightened credit recently and banks are not lending as freely as before. This drop in demand will be taking place just as supply is on the upswing, leading to what could be large losses for importers.

Insurance/Healthcare

- According to the Ponemon Institute's ninth annual Cost of Data Breach Study, sponsored by IBM, the average consolidated cost of a data breach increased by 15 percent in the past year to reach $3.5 million.

Financial Services

- Security researchers say the recent high-profile vulnerability affecting Microsoft's Internet Explorer browser was exploited by two separate state-sponsored groups in China. This time the attacks went after technology and energy firms in Europe and the U.S.

Global Intelligence

- Fox News reported that labor organizers are planning another day of fast-food protest slated for May 15, 2014 with coordinated actions expected in the US and more than 30 countries. Union representatives from countries including Argentina, Hong Kong, Italy, New Zealand and Panama gathered in New York this week to share tips and strategize for the demonstrations slated to take place on May 15. The protests calling for pay of $15 an hour in the U.S. have gained national media attention since they began in New York in late 2012.

Legal and Regulations

- The Department of Justice and the Federal Trade Commission on April 10 issued Antitrust Policy Statement on Sharing of Cybersecurity Information, a joint policy statement that provides critical infrastructure industries the clarity they need to share cybersecurity information among themselves to combat cyber threats without violating the antitrust laws those agencies enforce. The agencies note that “properly designed cyber threat information sharing is not likely to raise antitrust concerns and can help secure the nation’s networks of information and resources.”

Energy

- The Indie Fest Annual Humanitarian Award was awarded to a smart meter documentary film, “Take Back Your Power.” Filmmaker, Josh del Sol investigates the smart meter technology being deployed by utilities and governments. He claims their use is to “harvest data from private homes and introduce new pricing schemes. Commentary from whistleblowers, government agents, lawyers, environmentalists and doctors claim to “exposes corporate corruption and the erosion of human rights in the name of ‘going green’.” Indie Fest Coordinator Thomas Baker, PhD stated, “Take Back Your Power takes on the daunting yet important task of educating people worldwide about the surveillance, hacking, health, home safety, and consumer cost concerns linked to so-called ‘smart’ utility meters. It was selected out of hundreds of films for our Annual Humanitarian award because it delves into the heart of what is possibly the main problem in our world today: corporations taking over without conscience, and causing extreme levels of harm in the process.”

- The Union of Concerned Scientists are supporting a campaign for all citizens to write to their Governors to demand a “more climate resilient electricity system.” The group wants to know what each state is doing to prepare the electricity sector for the impacts of
global warming. “Urge your governor to conduct a state-wide vulnerability assessment that identifies the risks of extreme weather and climate change to the electricity sector and to increase your state’s use of renewable energy and energy efficiency.”

- Students of Washington University were arrested in St. Louis as they attempted to enter the quarterly meeting of the Board of Trustees at Peabody Energy. The action followed a historic 17-day sit-in at the St. Louis campus, where hundreds of Washington University students have joined in a campaign to remove Peabody Energy CEO Greg Boyce from the Board of Trustees, as part of other demands to cut university ties with the coal industry giant. “Today’s arrests are part of a larger fight against Peabody Coal in St. Louis, across the country, and around the world,” said Caroline Burney, with Students Against Peabody Energy. “We’re here for ourselves and for all of the other communities that Greg Boyce and Peabody Coal have destroyed, including including Rocky Branch, Illinois and Black Mesa, Arizona.”

- Activists will be holding the 2nd annual Hands Across the Sand event on May 17. This is a National Day of Action held in beach locations on multiple continents in order to protest pipeline, export and offshore energy projects.

- The No Pipelines! Action Camp for Climate Justice will be held from June 3-6 in Monkton, VT.

- The Sierra Club is circulating a petition for Ohio Gov. Kasich to veto the state’s new clean energy bill.

**Agribusiness**

- Fast food worker’s global protest coming up. So far, leaders from Argentina, Hong Kong, Italy, New Zealand and Panama have gathered to discuss plans. The demonstrations will be held May 15.

- Due to recent crackdowns from the Chinese government, it is forecast that palm oil imports from the world’s #2 importer will fall. Palm oil had been a commodity that was commonly used for financing in China, but the government has tightened credit recently and banks are not lending as freely as before. This drop in demand will be taking place just as supply is on the upswing, leading to what could be large losses for importers.

**Insurance**

- The chairman of a House committee has requested that the Government Accountability Office conduct a “complete and continuous end-to-end testing” of the security of the HealthCare.gov site and systems. But federal officials say extensive testing of the site is ongoing.

- As an ongoing process, regular audits are a necessity for any environment, especially those that are highly regulated, like healthcare. At the very least, on a quarterly basis, managers and system owners should be asked to review access privileges and attest that the current rights meet established internal requirements.

- Baylor Regional Medical Center at Plano reported a breach to HHS that affected 1,981 patients. On February 24, 2014, BRMC learned that “phishing” emails were sent to a small group of affiliated physicians who responded to the emails thinking that they were legitimate internal requests on or after January 23, 2014. By responding to the “phishing” email, the affiliated physicians may have inadvertently created an opportunity for unauthorized access to their email accounts.
- Molina Healthcare of New Mexico recently began notifying 5,261 former members that their protected health information (PHI) had been exposed by mistake. Creel Printing, which was hired by Molina to print postcards to be sent to former Molina members, mistakenly printed some former members' Social Security numbers (SSNs) on the postcards.

- According to the results of a recent survey of 102 financial organizations and 151 retail organizations in the U.K., 35 percent of respondents said it would take more than two days to detect a breach of their systems. The survey, conducted by Atomic Research and sponsored by Tripwire, also found that 24 percent of respondents have already suffered a data breach that exposed personally identifiable information (PII), and 36 percent of respondents said they don't have confidence in their security incident response plan.

- The Department of Health and Human Services (HHS) announced Wednesday that it had handed out $4.8 million worth of HIPAA fines to New York and Presbyterian Hospital (NYP) and Columbia University (CU) after they submitted a joint breach report that dates back to September 27, 2010.

- The New York State Senate passed legislation Thursday to crack down on criminals and scam artists who commit auto insurance fraud that costs New Yorkers billions of dollars in higher insurance premiums, and has caused serious injuries and death to innocent victims. The bills, sponsored by Senator James Seward, Chairman of the Senate Insurance Committee, and Senate Coalition Co-Leader Dean Skelos, would significantly reduce auto insurance scams by increasing penalties for those who commit or assist in the fraud.

- The Nevada Highway Patrol warned Las Vegas Valley drivers Wednesday to be wary of potential scammers who show up at traffic crashes asking for personal information. The warning grew out of a trooper report made Monday indicating a man who was not involved in a crash showed up at the scene and indicated he was taking a vehicle collision report for police.

- At least nine Boulder Community Health patients have had copies of their personal medical records stolen either from inside or nearby the hospital’s Foothills campus, then mailed to them by an anonymous source. It’s the third such breach the hospital has investigated since 2008.

- UMass Memorial Medical Center (UMMMC) recently began notifying approximately 2,400 patients that their information may have been accessed inappropriately by a former employee.

- Indiana's DeKalb Health recently announced that some patient information may have been exposed when a server operated by the third-party vendor that runs its Web site "was the target of an overseas hacking attack."

- The CIO of Hastings Insurance Services, James Fairhurst, has been leading an anti-fraud initiative at the UK insurance company that has seen significant business benefits for the organization. A Broker Anti-Fraud team reports to Fairhurst and operates a grey list of customers with whom Hastings consider it not in its interests to do business.

- Outrage over the handling of Alberta’s largest-ever breach of private health information has prompted new legislation that will force companies to immediately raise the alarm if a similar incident happens again. Health Minister Fred Horne said amendments to the Health Information Act will require custodians of health information to disclose any breach to his office, the Information and Privacy commissioner, and every person potentially at risk from having their data compromised. Failure to comply could result in
fines of up to $10,000 for an individual and $500,000 for a company.

- According to the Ponemon Institute's ninth annual Cost of Data Breach Study, sponsored by IBM, the average consolidated cost of a data breach increased by 15 percent in the past year to reach $3.5 million.

- The Boston Globe reports that the Boston Medical Center (BMC) recently began notifying approximately 15,000 of its patients that doctors' notes containing their personal information had been posted without password protection on the Web site of a transcription service used by BMC physicians. The data exposed on MDF Transcription Services' Web site included patients' names, addresses, and medical information, including prescriptions, but did not include Social Security numbers or financial information.

- Larsen Dental Care is notifying the public of a recent incident which could result in possible exposure of certain types of information. On March 4, 2014, an external hard drive was stolen from an employee's vehicle. Through forensic analysis, it was determined that data on the stolen hard drive may have included information for persons such as name, address, date of birth, email address, phone number, dental record, medical history, health insurance identification number and Social Security number.

- Most healthcare cloud security discussions involve a cloud provider's willingness (or perhaps lack thereof) to sign a HIPAA business associate agreement (BAA). What was once considered an agreement that vendors didn't have much reason to sign, the HIPAA Omnibus Rule put teeth into regulatory responsibility among BAs, helping the BAA evolve into a bare minimum to do business with many healthcare organizations.

---

**Financial**

**Activism**

- Activists held an anti-capitalism protest at a leading U.S. bank's annual shareholders meeting in Charlotte, NC on May 7th.

- Activists held an anti-GMO protest near the Philadelphia Stock Exchange on May 9th.

- An environmental activist group launched a petition campaign against a leading U.S. bank regarding its fossil fuel investments, calling on the bank to "accurately report the climate change pollution it funds."

- Housing activists in Atlanta delivered a petition to a leading U.S. bank branch in Decatur, GA on May 8th, demanding that the bank stop foreclosing on homes.

- Activists held an anti-GMO industry protest in New York City, demanding that investment firms on Wall Street divest from agricultural biotechnology companies that produce GMO crops.

- Housing activists in Michigan announced a weekly action at the Bankruptcy Court in Detroit, MI denouncing foreclosures, evictions, and utility shutoffs. The action event will take place every Friday at 4:00 PM EDT.

- Housing activists will conduct a sit-in at a leading U.S. bank branch in Atlanta, Georgia on May 14th to demand the bank work out a deal with a local minority-owned construction company that's being foreclosed on.
A hacker group claimed to have leaked a total of 60,622 credit card accounts from multiple credit card brands.

A hacker group claimed that it will target U.S. banks with DDoS attacks during the collective's #TheWeekOfHorror operation set to launch in July 2014.

A hacker group published a list of 1,207 credit card numbers allegedly belonging to Georgian (country) citizens. The group also claimed to have 730,000 more accounts.

A tweet made last week by a known hacker group suggests ATMs owned by a leading U.S. bank may be targeted “on a holiday or Sunday.”

A Las Vegas company that owns casinos in four states says its system for processing credit and debit card information was hacked.

Researchers revealed a disabled account in Windows’ network does not take effect immediately. Due to design considerations, disabled accounts and deleted, expired, and locked-out accounts effectively remain valid up to 10 hours after they had supposedly been revoked. So-called disabled accounts expose the corporation to advanced attackers seeking to gain access to the corporate network.

Security researchers say the recent high-profile vulnerability affecting Microsoft's Internet Explorer browser was exploited by two separate state-sponsored groups in China. This time the attacks went after technology and energy firms in Europe and the U.S.

A coalition of nearly two-dozen tech companies and civil liberties groups is launching a new fight against mass internet surveillance, hoping to battle the NSA in much the same way online campaigners pushed back on bad piracy legislation in 2012. The groups are calling on developers to add at least one NSA resistant feature to mobile apps, and on websites to add security features like SSL (Secure Socket Layer), HSTS (HTTP Strict Transport Security), and Perfect Forward Secrecy to better secure the communication of users and thwart government man-in-the-middle attacks. They also want mobile apps and websites to post a Reset the Net splash screen on June 5 and are distributing a privacy packet for users that contains a bundle of various free software tools, like Adium and Pidgin (for encrypted chat), Textsecure, and Redphone (encrypted phone calls and text messaging) and GPG (for encrypted email).

A hacker group targeted the Central Bank of Syria with cyber-attacks.

An information technology security firm released a study that surveyed 200 IT and admins (100 in the energy sector and 100 in the financial service sector) and concluded that 72% of energy and financial service firms expect to be attacked by Advanced Persistent Threats (APT), targeted malware attacks or other sophisticated cybercrime or cyber-espionage tactic in the next 12 months.

Researchers say a new ransomware program called CryptorBit, which is similar to CryptoLocker and CryptoDefense, is being increasingly installed on Windows computers through fake flash updates and other social engineering tactics. Cryptocoin miner software which utilizes the victim’s computer to mine digital coins such as Bitcoin is also installed.

A UK spy agency has warned large corporations that foreign spy agencies may be secretly recruiting their IT workers in the hope of gathering sensitive information for use in cyber-attacks.
A hacker group threatened to target two leading U.S. banks with cyber-attacks on May 8th, likely using DDoS attacks.

Researchers say fraudsters are now targeting third-party payroll services. In this recent uptick in tax identity fraud, criminals have been targeting the HR departments of various organizations in order to get the W-2s of employees in order to file fraudulent tax returns.

**Legal, Litigation, Regulatory Risk**

- A Moroccan Hacker wanted by Swiss police for hacking banks in Switzerland was arrested by Bangkok police. Swiss authorities say the suspect and about 10 other accomplices had hacked bank accounts in Switzerland causing damage equivalent to more than 600 million baht before fleeing the European country.

- The U.S. Justice Department is pursuing criminal investigations of financial institutions that could result in action in the coming weeks and months, U.S. Attorney General Eric Holder said in a video, adding that no company was "too big to jail."

- The U.S. Federal Reserve proposed a rule that would prohibit a bank merger if the new company's liabilities exceed 10% of the aggregate consolidated liabilities of all financial companies. Companies subject to the rule would be depository institutions, bank holding companies, savings and loan holding companies, foreign banking organizations, companies that control insured depository institutions, and non-bank financial companies designated "as systemic" by the FSOC.

**Operational Risk**

- Due to unspecified technical problems, trading on the Philippine Stock Exchange was halted an hour before the noon break on May 5th.

- Bitcoin's first exchange in India debuted with the name BTCxIndia on May 6th. The site is said to provide a secure, real-time trading platform adhering to KYC and AML guidelines and enables instant INR deposits and withdrawals.

- The US Federal Exchange Commission (FEC) has determined that political campaigns and political action committees (PACs) may accept bitcoin as a form of in-kind donation under current federal election laws. The FEC also determined that campaigns are required to adhere to existing guidelines for reporting the receipt or sale of bitcoins. This includes collecting personal information from donors.

- An article published last week argued Russia's development of its own payment system and its punitive moves against leading credit card brands may set a precedent, and encourage more countries to develop domestic payment programs to protect against the possibility of sanctions or other international disruptions.

**Reputational Risk**

- A petition launched on the website of a progressive public policy advocacy group encourages supporters to prevent a leading U.S. bank from claiming their settlement with the Department of Justice for mortgage lending abuses as tax deductible.

- Tweets circulated last week among activists claimed that a leading U.S. investment bank is "buying up homes everywhere" and "getting homes for pennies on the dollar."

- A petition launched on the website of a nonpartisan grassroots activist organization calls for the House and Senate Ethics Committees to investigate Wall Street lobbyists who are allegedly "writing the laws that are supposed to be regulating Wall Street."