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

- Thirty states run their own railroad inspection programs to supplement federal inspectors stretched thin nationwide. Several of them, including Minnesota and New York, are trying to add inspectors to cope with the influx of trains hauling North Dakota crude. In North Dakota, state officials are just realizing that's an option. The state has left inspections of tracks, tank cars and rail-loading facilities to federal regulators, whose ranks in the region haven't grown even as crude-by-rail shipments out of the Bakken have increased from fewer than 100,000 barrels a day in 2010 to 800,000 barrels per day late last year.

Agribusiness
A petition circulated in Mexico by the Union of Scientists Committed to Society asks that President Enrique Pena Nieto ban GMOs in Mexico. The group intends to collect as many as 1 million signatures. As of the writing of this report it had collected nearly 3,500, many from doctors, scientists, and students.

Insurance/Healthcare

- The Security Industry Association has released a new Privacy Framework with the intent of helping healthcare organizations and vendors identify a set of privacy principles to serve as a guide for manufacturers, integrators and distributors of electronic security technologies; inform policymakers about how the security industry protects patient privacy; and educate end users on patient privacy.

Financial Services

- U.S. Federal regulators warned April 3rd of a trend involving thieves hacking ATMs to withdrawal large amounts of money, circumventing ATM’s monetary withdrawal limits. The hackers steal account information directly from banks, then often wait for weekends and holidays when the ATMs are fully loaded with cash to hack into the software that runs ATMs to remove any cap on withdrawals. Hackers netted more than $40 million to date running this scam.

Worldwide Intelligence

- The German District Attorney’s Office of Verden (Lower Saxony) has discovered a data set of 18 Million compromised email addresses including passwords. Apparently, the data set looks recent and some of the compromised accounts are currently used by criminals, e.g. to push spam. Accounts from across all major German email providers are said to be compromised.

Energy

- A coalition of local, statewide and national groups concerned about toxic waste from fracking, gathered yesterday at the Ohio statehouse for “Don’t Waste Ohio” Legislator Accountability Day. The coalition called for an end to Ohio being used as a regional dumping ground for oil and gas waste. Participants attending the accountability day met with their legislators in the morning and attended a rally in the afternoon advocating for the passage of legislation in both the House and Senate that would ban fracking wastewater injection wells.

- For the first time, members of Congress today called upon U.S. Environmental Protection Agency (EPA) Administrator Gina McCarthy to “investigate and address the water contamination” in Dimock, PA, in Parker County, TX, and in Pavillion, WY. In all three communities, the EPA has previously withdrawn investigations into water contamination and stopped providing affected residents with clean drinking water. Eight Representatives, led by Rep. Matt Cartwright (PA-17), made the request in a letter to Administrator McCarthy.

- Methane emissions have decreased by 11 percent in the past 24 years, but they could pick back up by 2030 if actions aren’t taken to combat them. That’s why the powerful greenhouse gas is the center of a newly announced strategy by the White House. Released Friday as a new layer to President Barack Obama’s Climate Action Plan, the methane emissions strategy aims to bring economic and health benefits to the country while fighting climate change by removing a gas from the atmosphere that, by the ton, has about 20 times the global warming effect of carbon dioxide.
Article reports that "Pennsylvania’s farm lobby is throwing its support behind a bill aimed at limiting the ability of gas companies to withhold royalty money from landowners. As StatelImpact Pennsylvania has previously reported, the state’s largest driller–Chesapeake Energy– has been widely accused of shortchanging landowners who have leased their property for gas development. A bill currently in the state House would amend Pennsylvania’s 1979 Guaranteed Minimum Royalty Act. It’s an effort to protect landowners from royalty deductions known as “post-production costs”—the expenses incurred in processing and transporting gas.”

Forest and Bird has issued a press release announcing that the sell-off of deep-sea drilling rights in some of New Zealand’s deepest waters and onshore oil and gas drilling and fracking rights in some of New Zealand’s most valuable areas of native forest could come at a huge cost to New Zealand’s natural heritage.

Jonathan Libber, president of Maryland Smart Meter Awareness (MSMA) filed a motion for reconsideration with the Maryland Public Service Commission’s (PSC) regarding its opt out Order of February 26th. Although the Order provided Maryland ratepayers the right to officially opt out from having a smart meter installed on their homes, MSMA submits that BGE, Pepco, Delmarva Power & Light and SMECO never justified their claim for substantial opt out fees. MSMA was the only involved party that raised very strenuous objections to the cost analyses presented to the PSC by the utilities.

Newfoundland Power’s Michelle Coughlan says they’re deeply disturbed by an act of vandalism that left thousands without power in the middle of a snowstorm yesterday. A vandal shot at the Pulpit Rock Substation in Torbay early yesterday morning, leaving 5,000 customers without power and causing an oil spill. Newfoundland Power is offering $5-thousand dollars to anyone who can identify the person responsible. On VOCM’s Nightline with Jonathan Richler last night, Coughlan said the oil spill has been contained and now they are focusing on the clean-up.

Citing the sharp increase in the transportation of crude oil by rail, a group told Congress on Wednesday that most of the country’s fire departments lack sufficient training to respond to hazardous materials incidents. Elizabeth Harman, assistant to the general president for training and grants at the International Association of Fire Fighters, said recent funding cuts have hurt efforts to train firefighters at the proper level and keep them updated on new hazards. “There are significant portions of the country where first responders are not prepared for an incident involving hazardous materials,” said Harman, a certified fire service instructor. Harman told the House of Representatives Subcommittee on Railroads, Pipelines and Hazardous Materials that 65 percent of fire departments that respond to hazardous materials incidents have not trained all of their personnel for it. “This is an untenable situation that must be rectified,” she said.

Thirty states run their own railroad inspection programs to supplement federal inspectors stretched thin nationwide. Several of them, including Minnesota and New York, are trying to add inspectors to cope with the influx of trains hauling North Dakota crude. In North Dakota, state officials are just realizing that’s an option. The state has left inspections of tracks, tank cars and rail-loading facilities to federal regulators, whose ranks in the region haven’t grown even as crude-by-rail shipments out of the Bakken have increased from fewer than 100,000 barrels a day in 2010 to 800,000 barrels per day late last year. But the explosive derailment in Casselton on Dec. 30 was a wake-up call for North Dakota officials, regulators and lawmakers to just how much oil is being shipped by rail, how volatile Bakken crude may be and what little has changed to oversee its transport. Now, they say, it might be time for North Dakota to get involved and put its own inspectors in the field. Gov. Jack Dalrymple and a member of the state’s Public Service Commission said last week they will spend the next few months looking into whether the state should set up its own program.
Agribusiness

- La Via Campesina is intensifying organization for an international, with protests set to take place across Europe (especially France and Belgium) and South America. La Via Campesina is affiliated with several large agricultural reform groups in countries across the world – notable members include the MST in Brazil, the MCP in Paraguay, and the Confederation Paysanne in France. This year’s protests will center on a theme of “indigenous seed freedom”, with the group expressing opposition to seed patent laws, and it is likely that groups involved in the protest will target entities whose business models revolve around patenting seeds.

- The MST reports that the Federal Public Ministry in Mato Grosso, Brazil, has proposed a “civil action” against the state and the Institute of Agribusiness Defense to prohibit the use of pesticides containing emamectin benzoate.

- RT and several Russian news outlets reported on April 6 that Prime Minister Dmitry Medvedev has announced that Russia will not import GMO products, ordering “widespread monitoring of the agricultural sector” to enforce the measure.

- A petition circulated in Mexico by the Union of Scientists Committed to Society asks that President Enrique Pena Nieto ban GMOs in Mexico. The group intends to collect as many as 1 million signatures. As of the writing of this report it had collected nearly 3,500, many from doctors, scientists, and students.

Insurance

- A new survey of CIOs finds that healthcare organizations lag behind those in other business sectors when it comes to having a formal mobile technology strategy.

- The recent discovery of malware on a server storing health data used for research has prompted Kaiser Permanente to contact 5,100 patients about a potential privacy breach. Patient information that was contained on the server, or in a file connected to the server, includes name, date of birth, age and gender, and possibly address, race/ethnicity, medical record number, lab results associated with research, and responses individuals provided to research-related questions.

- The Security Industry Association has released a new Privacy Framework with the intent of helping healthcare organizations and vendors identify a set of privacy principles to serve as a guide for manufacturers, integrators and distributors of electronic security technologies; inform policymakers about how the security industry protects patient privacy; and educate end users on patient privacy.

- La Palma Intercommunity Hospital has notified patients that their medical records and personal information may have been illegally viewed by a former employee. The hospital learned in September 2012 that an employee accessed personal information without permission, including Social Security numbers, driver’s license numbers, addresses, birth dates, and limited medical information.

- Sutherland Healthcare Solutions, who disclosed a breach affecting over 220,000 patients in California, discovered that additional patients had information on the stolen computers and is now sending them notification letters. Los Angeles County officials said Thursday that 170,200 additional victims have been identified in a theft of medical data from a county contractor’s office. The total number of county patients affected now stands at 338,700.
• The Michigan Department of Community Health (MDCH) recently became aware of a breach of protected health information under the Health Insurance Portability and Accountability Act (HIPAA) and is notifying 2,595 individuals and the Department of Health and Human Services regarding this breach.

• Hospital records have been sold to dozens of companies, including pharmaceutical giants and private firms, without patients' knowledge or consent, newly-released data shows. Details about NHS patients have gone to major names, including Bayer, Baxter, AstraZeneca, Bupa and Roche.

• California's Palomar Health recently began notifying more than 5,000 patients that their personal and medical information may have been exposed when two unencrypted flash drives were stolen from an employee's car on the evening of February 21, 2014.

• The Security Industry Association has released an updated version of its privacy framework, outlining best practices to use when deploying evolving electronic security technologies. "We needed to update the framework to reflect the fact that a lot of security systems are IP-based now and connected online," says Jake Parker, director of government relations at the SIA, a trade association for electronic and physical security solution providers with more than 450 member companies. The original framework was released in 2010.

• A nonprofit advocacy group for children with developmental disabilities is notifying 2,934 families of a potential data breach that occurred when someone stole computers from the group's Austin office. The computers contained clients' birthdates, Social Security numbers, Medicaid numbers, photos and health information.

• University of Kentucky HealthCare (UK HealthCare) recently began notifying 1,079 patients that their protected health information (PHI) may have been exposed when a third-party vendor's password-protected laptop was stolen on February 4, 2014.

• Although open enrollment season for health insurance coverage under the Affordable Care Act has ended, skepticism about the security and privacy protections for data on the HealthCare.gov website and systems continues.

• A recent survey of 268 IT decision makers, including senior management, security managers, directors, and network and systems engineers, found that 71 percent of respondents said they're either "not confident" in their security or "not at all prepared" to manage a potential security breach.

• Billing vendor PracMan recently began notifying several clients' patients that their personal and medical information may have been exposed when an IT subcontractor mistakenly copied and stored files on an unsecured server.

• The biggest identity and access management challenges for healthcare providers are being able to manage clinical data access on a granular basis and make sign-on simple but secure for clinicians, says security expert Mark Ford.

• Tacoma's Franciscan Health System is notifying some 8,300 patients that their personal information — including in some cases medical records and Social Security numbers — may have been shared with computer scammers who accessed staff email accounts. Franciscan estimates more than 12,000 patients nationwide had files potentially breached.

• More than 30.6 million individuals have been affected by major healthcare data breaches since September 2009, according to the latest tally from federal regulators. And looking ahead, some security experts believe that the nature of many large breaches will shift, with business associates being implicated more often.
Financial

Activism

- Occupy affiliated Wave of Action campaign events targeted multiple bank brands in New York City on April 4th, consisting primarily of protest activity.

- Demonstrations will occur at U.S. Embassies on April 15th (Tax Day) to demand the U.S. end support of the Israeli occupation Of Palestine as organizers claim “U.S. taxpayers pay unknowingly $4-6 billion to support Israeli apartheid while the USA government obstructs justice by using its Veto power against the application of International laws.”

- An activist group plans a 'Taking Back Our Schools' rally and march to occur on May 17th at New York City Hall Park where participants will demand the creation of "a public school system that provides a fully funded, equitable, community-based education for every child.”

- Occupy Wall Street supported a labor union’s 'March4TheDream' event in New York City on April 4th in which airport sanitation workers marched from JFK Airport to LaGuardia Airport.

- A 'Low Wage Worker MLK' rally occurred April 3rd in West Park, FL.

- Occupy activists protested the Supreme Court's McCutcheon vs FCC campaign finance decision with actions at NYC's City Hall Park, and in Chicago, IL's Federal Park, on April 2nd. Participants claimed the ruling undermines democracy by making it easier to bribe politicians.

- Housing activists continue to engage in weekly protests outside a leading U.S. investment bank’s branch in Seattle, WA for perceived unjust foreclosure practices.

Information Security Risk

- A new malware family, CRIGENT (also known as “Power Worm”) is targeting Word and Excel files (detected as W97M_CRIGENT.JER and X97M_CRIGENT.A). Most significantly, instead of creating or including executable code, CRIGENT uses the Windows PowerShell to carry out its routines. IT administrators that are normally on the lookout for malicious binaries may overlook this, as malware using this technique is not particularly common.

- A security firm traced a new rash of credit and debit card scams involving bogus sub-$15 charges to a company called “BLS Weblearn.” The security firm states BLS Webleam is part of a prolific international scheme designed to fleece unwary consumers.

- An established hacktivist collective continues to attack Saudi-based banking websites with DDoS attacks.

- Offers for fake “Bitdefender Antivirus Plus 2015” free software downloads are circulating YouTube and Facebook, which actually downloads malicious software.

- A security firm published a report that concludes about 99% of malware attacks are based on incremental tweaks to existing malware and method. The report analyzed more than 4.1 billion live attacks and found most attackers use exploit kits today. The firm detected some 67 million attack attempts via exploit kits last year. Blackhole was the most popular kit in use for much of 2013, but after its alleged creator “Paunch” was arrested in October, Magnitude and Redkit have been battling it out for the No. 1 slot.
• U.S. Federal regulators warned April 3rd of a trend involving thieves hacking ATMs to withdraw large amounts of money, circumventing ATM's monetary withdrawal limits. The hackers steal account information directly from banks, then often wait for weekends and holidays when the ATMs are fully loaded with cash to hack into the software that runs ATMs to remove any cap on withdrawals. Hackers netted more than $40 million to date running this scam.

• A malware security company reports the infamous Zeus banking Trojan was responsible for 38% of banking trojan activity in 2013, and, that a host of new Zeus variant releases have made it more likely for Zeus to infect a machine on networks.

• An ISP security group discovered that a large amount of the DNS DDoS amplification attacks of 2013 probably had a previously undetected helping hand from millions of poorly-configured home routers. Using figures from its own network, the firm estimates that as many as 24 million home routers across Asia, parts of Eastern Europe and Central America could be operating as open DNS proxies, with 5.3 million detected as having been used in DDoS attacks in February alone.

Legal, Litigation, Regulatory Risk

• Two U.S. banks filed a class action lawsuit against a leading U.S. retailer who suffered a massive data breach a few months ago that resulted in over 100 million compromised payment card details and other personal records.

• U.S. regulators are seeking ways to prevent high-frequency trading abuses without blocking high-speed firms that may actually benefit investors by providing liquidity to the markets. Regulators are looking into whether those traders are breaking U.S. laws by acting on nonpublic information.

Operational Risk

• The Occupy National Gathering will be held in Sacramento, CA from July 31st through August 3rd. The purpose of the event is to discuss Occupy's initiatives for the upcoming year.

• A recently published study finds that businesses around the world are counting the cost of failing to defend against advanced evasion techniques (AETs), as nearly 40% of CIOs and security managers whose organizations were breached by cyber-attacks on their networks believe AETs played a key role. The study polled 800 CIOs and security managers in the UK, US, Germany, France, Australia, Brazil and South Africa. On average, respondents said breaches in the past 12 months have cost around $931,000, with the financial sector hardest hit. The cost is estimated at more than $2m per breach globally.

Reputational Risk

• A New York based lobbyist group and Occupy members held an organizers’ meeting for various organizations and groups opposed to Governor Andrew Cuomo’s “anti-people and regressive 1%” agenda on April 4th at Federal Hall, 26 Wall Street, in NYC. The event consisted of a rally, speak out, and march to Zuccotti Park.

Global Intelligence
Germany

- The German District Attorney’s Office of Verden (Lower Saxony) has discovered a data set of 18 Million compromised email addresses including passwords. Apparently, the data set looks recent and some of the compromised accounts are currently used by criminals, e.g. to push spam. Accounts from across all major German email providers are said to be compromised.

Japan

- Japanese Defense Minister Itsunori Onodera issued a “destruction order” for any missiles launched by North Korea toward the Sea Of Japan, in response the country’s launch on March 26 of 2 Rodong missiles. Onodera stated that the move is to prevent any missiles from reaching Japan.

North America

- Gamespot reported that after Microsoft promoted Phil Spencer to the new position of Head of Xbox, Microsoft has cut an unspecified number of positions.

- KTVU News reported that the San Francisco Board of Supervisors has denied an appeal that would have stalled the start of a pilot program for private commuter shuttles. The 18 month program would charge private shuttles $1 per stop to use designated Municipal Railway bus stops. The program was approved by SFMTA board of directors in January and is slated to begin 7/1/2014.

- Wopular reported that CWA says that Sprint might owe millions to its recently laid off employees. The union claims that Sprint violated federal law with the layoffs and could owe $4.5 million in back pay to 1,440 workers laid off in March.

- The LGBTQNation reported that sponsors of a ballot measure to legalize gay marriage in OR asked a federal judge on 4/1/2014 to make a speedy ruling in a case that challenges the state’s ban on same-sex weddings.

- Notorious hacking group “Nullcrew” has continued its spree of leaking email credentials from major media companies. In the past week, NullCrew joined forces with famed hacking group and Anonymous affiliate “TheHorsemen” to attack Al Arabiya, a major Middle Eastern media company. Communications of journalists, executives and media sources have all been exposed in the attack, which was purportedly carried out by exploitations in the company’s mail servers. According to the pastebin.com post that leaked the information, Al Arabiya’s email server software was due for a security patch update in December 2013 but was never updated.

Vietnam

- Lao Dong News, a local VNese media source, reported that nearly 100 workers from Lua Vang company, a chemical manufacturing plant, went on strike on 3/27/2014. According to the workers the company only allowed workers 1 bathroom break and each break can only last 7 minutes. Workers who went more than the allotted time had their wages deducted. In addition, workers have to have bathroom passes to go to the bathroom. With only 2 passes for over 30 people, it takes a long time before workers can actually take bathroom breaks. Workers also complained that the company failed to follow regulations because it did not workers a copy of the contract, the company increased overtime hours without consulting workers, and any new policies instituted by the company would involve the deduction of workers’ wages. For example, workers that took leave had their salary deducted, workers that took sick leave had their salary deducted, workers that didn’t work overtime had their salary deducted.... The company representative stated that they have followed regulations and workers are allowed 1 bathroom break every 4 hours. According to the company, every company in the area
has the same bathroom break policy. According to the newspaper, the company has already recruited 70 new workers and old workers anticipate to be let go over this incident.