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
- Pharmaceuticals
- Retail
- Technology
- Telecommunications
- Entertainment
- Defense
- Law Enforcement

Register Now for our December Webcast

Making the Business Case for Threat Intelligence

December 17, 1 pm ET

To adequately protect company assets and ensure business continuity in the face of today’s threats, organizations must be more proactive. Fortunately, many outside threats, actors and methods can be detected and studied in advance through open source Internet monitoring and intelligence analysis. In this webinar, we’ll discuss how you can make a practical case for deploying threat intelligence in your organization.

Top Incidents

Energy

- The Peruvian government plans to file criminal charges against Greenpeace activists who may have permanently scarred the Nazca Lines World Heritage Site when they entered the area laying big yellow cloth letters reading, “Time for Change! The Future is Renewable.” The Nazca lines are between 1,500 and 2,000 years old depicting figures that can only be seen from the air. The ground is so sensitive and so sacred that Peru has even forbidden presidents and top officials to walk where the Greenpeace activists went.
**Agribusiness**

- On Thursday, December 11, 2014 dairy farmers drowned politicians' portraits in milk in a protest against plunging prices. More than 350 farmers from 10 countries joined the European Milk Board’s demonstration outside the offices of the EU Commission in Brussels. Farmers filled a lake of milk containing pictures of European leaders like German chancellor Angela Merkel, French president François Hollande and EU farm commissioner Phil Hogan. They then set fire to straw bales in the middle of the street.

**Insurance/Healthcare**

- The National Health Information Sharing & Analysis Center is making available for free to its members a new intelligence platform that aims to help ease cyberthreat information sharing. The introduction of the new NH-ISAC Threat Intelligence Platform comes as another healthcare industry organization, the Health Information Trust Alliance, is also gearing up to release a previously announced cyber-alert system for the sector in January.

**Financial Services**

- Cybercriminals are using a new variant of the Neverquest malware to target the customers of financial institutions worldwide. The banking Trojan was first spotted in November 2013, and the threat is believed to be an evolution of the Snifula malware family. New variants of Neverquest were released this summer with most infections spotted in the United States and Japan.

**Global Intelligence**

- A Chinese news outlet reports 1.5 million Wi-Fi passwords have been stolen from a Shanghai company that develop Wi-Fi Hotspot Application. According to the article, the hackers exploited Wi-Fi sharing applications to remotely control by injecting malicious codes to these applications and turned users devices to bots.

**Legal and Regulations**

- On December 10, 2014, the New York Department of Financial Services (NYDFS) issued a letter to banking institutions chartered or licensed in New York notifying them of an expansion of the NYDFS information technology examination procedures to focus on cyber security issues as an integral aspect of risk management. The expanded procedures will look at cyber security in a comprehensive manner and will include a review of corporate governance as it relates to cyber security risks, the relationship between information security and core business functions, shared infrastructure risks, training, disaster planning and insurance coverage and other third-party protection.

**Pharmaceuticals**

- Drug makers and Internet companies are quietly working together to link U.S. pharmacy records with online accounts in order to target ads to people based on their health conditions and their prescription drugs, Bloomberg News writes. In a little-known process, third-party companies assign patients unique numerical codes based on prescription records, a practice websites also rely on to track their registered users, the news service writes. The data sets, Bloomberg explains, can be linked without names changing hands, allowing drug makers to identify who uses a specific medicine and to send customized Internet ads. The practice has become an essential part of digital marketing efforts by drug makers, according to Bloomberg. But while the industry says the technique complies with federal medical privacy laws because patient names are concealed, critics see a breach of confidentiality.

**Retail**

- Earlier this month, security researchers discovered a new PoS malware family, which they named “LusyPOS” after a reference in Russian underground forums. We detect this
as TSPY_POSLUSY.A. In their analysis, they mentioned that it had some characteristics linked to the Dexter family of PoS malware. It also had behavior similar to the Chewbacca PoS malware (which we detect as TSPY_FYSNA.A), which is known to use the Tor network to connect to its command-and-control (C&C) servers.

**Technology**

- A growing number of flaws in web browsers is viewed as the biggest endpoint security headache by today’s IT decision-makers, according to Malwarebytes. With the number of exploitable browser vulnerabilities accelerating this year, 72% of the 685 IT decision-makers questioned said this made security difficult in their organization, more so than any other issue.

**Telecommunications**

- Where the U.S. eventually lands on the issue of net neutrality could have wider reaching international implications, including the possibility of opposition from the U.N. and World Trade Organization (WTO).

**Entertainment**

- Fallout from the Sony hack has continued after reports that sensitive contracts, unpublished scripts and salaries of top executives were leaked online. A recent email paper chain between two high-level executives disclosed an internal battle regarding the movies “Jobs” and the in development Angelina Jolie film “Cleopatra.” This is just the latest of what may be many devastating leaks following the recent data breach on Sony.

**Defense**

- A sophisticated cyber-espionage campaign believed to be the continuation of the Red October operation has been identified to target specific users of Android, iOS and BlackBerry mobile devices through spear-phishing attacks. Researchers from provider of security and network solutions Blue Coat have uncovered the endeavor that leverages a complex infrastructure relying on “a convoluted network of router proxies and rented hosts, most likely compromised because of poor configurations or default credentials,” to deliver targeted malicious emails. In an extensive report on Inception/Cloud Atlas, Blue Coat revealed that the threat actor planned attacks on mobile devices of high-profile targets in different sectors, from finance and oil industry to military, engineering and politics, in different parts of the world.

**Law Enforcement**

- With widely watched amateur videos of police killings as a backdrop, New York City police are hoping to arm more officers with stun guns as an option for subduing emotionally disturbed people and other suspects who resist arrest. Preliminary plans call for 450 additional officers to carry the electroshock weapons while on patrol, police officials said. The department would first have to find funding and develop more precise guidelines on which circumstance are appropriate to use the devices.

**Energy**

- The Sierra Club is organizing an anti-coal rally at the December 17, 2014 PUC meeting in Columbus, OH.

- The advocacy group PennEnvironment has released a report critical of drilling on public lands.

- The US Chemical Safety Board urged Congress to adopt safety and oversight standards modeled after the reforms California implemented following a 2012 refinery fire.
• Bloomberg reported that a 2008 pipeline explosion in Turkey was actually an act of cyberwar, and emphasized the vulnerability of US pipelines to such an attack.

• The Peruvian government plans to file criminal charges against Greenpeace activists who may have permanently scarred the Nazca Lines World Heritage Site when they entered the area laying big yellow cloth letters reading, “Time for Change! The Future is Renewable.” The Nazca lines are between 1,500 and 2,000 years old depicting figures that can only be seen from the air. The ground is so sensitive and so sacred that Peru has even forbidden presidents and top officials to walk where the Greenpeace activists went.

• On December 9, 2014 several dozen activists protested outside the office of the federal Bureau of Land Management in Reno Nevada in opposition to an auction of huge tracts of public land for private oil and gas exploration that they claim damages the environment and guzzles water in a time of drought. Protesters wore blue and carried empty jugs to signify the loss of water. The coalition included, environmentalists, ranchers, Native American leaders and real estate agents.

• Cove Point MD was the site for a three day protest by local, state and national environmental activists joined together against the construction of an export facility for natural gas obtained through fracking on Maryland’s Eastern Shore. Nine individuals were arrested at the demonstrations. Opponents fear the FERC’s “rubberstamping” of fracking projects could lead to increased fracking as companies attempt to keep up with foreign demand.

• December 11, 2014 started a week of pipeline protests across southern New England in advance of a decision to expand a natural-gas pipeline in the region. The Week of Respect and Resistance is a multi-state resistance to Spectra’s Algonquin Incremental Market (AIM) pipeline expansion through New York, Connecticut, Rhode Island and Massachusetts. The events are timed to coincide with the scheduled Dec. 19 release of an environmental report on the project by the Federal Energy Regulatory Commission (FERC).

• According to the Wall Street Journal, pipeline opposition is getting expensive. Keystone XL pipeline as well as another half dozen projects valued at $15 billion have been delayed by activism. The WSJ analysis show there's opposition to another 5,100 miles of pipeline, worth $25 billion, although protests haven't shut them down yet. Those might sound like big numbers, but it's just a fraction of the pipeline slated to be built in the next two decades. As Inside Energy reported earlier this year, by one estimate, half a million miles of pipeline will be built in the United States by 2035 -- enough to wrap around the Earth 22 times.

• Eco Watch reports that Wisconsin congressman Mark Pocan, with Illinois Congresswoman Jan Schakowsky, introduced a bill yesterday to ban fracking on publicly owned lands. Currently, 90 percent federally managed lands are available for oil and gas leasing, including fracking, with just 10 percent protected exclusively for conservation, recreation, wildlife and cultural heritage. The support for the new legislation came not just from environmental groups, but from those concerned with a wider range of economic and social justice issues, as well as health issues.

• World Nuclear News reports that Russia is willing to help India build “more than” 20 new nuclear power units, Russian President Vladimir Putin said last week following talks in Delhi with Indian Prime Minister Narendra Modi. A package of intergovernmental and interdepartmental documents was signed on the sidelines of the visit, including on cooperation in the energy, medicine, investment and humanitarian areas. Modi said that the two countries had set out an "ambitious vision" for nuclear energy during the talks and that the new reactors would be built over the next 20 years.

• The CBC reports that a U.S. cabinet member has cited aboriginal lands as a concern as her colleagues in the Obama administration near the completion of a review into the Canadian oil project. The secretary of the interior laid out that concern in an interview. "I think the fact that tribal nations are standing up saying, 'We're concerned about this.
We're concerned about water quality. We're concerned about tribal sovereignty. We're concerned about what this pipeline may do for our lands and our rights,' needs to be heard," Sally Jewell said.

- The Church of England has warned it could withdraw its investments from BP and Shell unless the oil giants take greater action to tackle climate change. In a significant boost to the growing "divestment" campaign that has spread from the US, the Church has become the first mainstream religious organisation in the UK to raise the prospect of severing ties with fossil fuel companies because of global warming.

- Tens of thousands of protesters brought Dublin to a standstill in a mass protest against Ireland's planned new tax on household water supplies, the last major measure in the country's six-year austerity drive. Police estimated more than 30,000 people attended the main "Right2Water" rally on Wednesday in the square outside the office of Prime Minister Enda Kenny, where socialist and nationalist politicians appealed from a makeshift stage for the public to boycott their water bills.

- At the United Nations Climate Change Conference in Lima, Peru, protesters gathered inside the building on Monday to protest the invitation of oil giants Shell and Chevron to speak on summit panels.

- An article on http://royaldutchshellplc.com states that the Opec oil cartel no longer exists in any meaningful sense and crude prices will slump to $50 a barrel over the coming months as market forces shake out the weakest producers, Bank of America has warned. Revolutionary changes sweeping the world's energy industry will drive down the price of liquefied natural gas (LNG), creating a "multi-year" glut and a much cheaper source of gas for Europe

### Agribusiness

- Congress will have to resolve the international snarl over U.S requirements for labels on beef, pork and chicken meat that identify where the animals were born, raised and slaughtered, said Agriculture Secretary Tom Vilsack.

- The chief U.S. agricultural trade negotiator said there was "a lot of momentum" toward a Trans-Pacific Partnership pact after months of delays. The chief negotiators from the 12 TPP nations are in Washington this week, said Darci Vetter, of the U.S. Trade Representative's office. "We hope and think we will be closing this agreement soon."

- CFTC chairman Timothy Massad said his agency, the regulator of futures exchanges, would focus on threats of cyber attacks on the derivatives industry, said Reuters, which quoted him as telling the Senate Agriculture Committee, "The risk is apparent." Massad said the CFTC "will focus on cybersecurity as it conducts compliance exams for exchanges and clearinghouses to make sure they are protecting themselves from cyber attacks," said Reuters.

- The Center for Food Safety reported that in Portland, Oregon citizens whose votes were not counted filed a lawsuit in the Circuit Court of the State of Oregon to ensure that their votes and those of approximately 4,600 others are not unfairly rejected. Oregon is currently undergoing a mandatory statewide hand recount of Measure 92, the genetically engineered (GE) food labeling initiative. With more than 1.5 million votes cast, the difference was less than a tenth of a percentage point (812 votes). The lawsuit, also brought by the Oregon Right to Know Campaign, asks the Court to direct the Secretary of State to count 4,600 ballots currently rejected without evidence of fraud or forgery.

- Endo Riot reported that China is blocking US imports over GMO contamination. Due to the recent contamination of hay from RoundUp ready GMO alfalfa, the Chinese government has now blacklisted hay from the US, and they are looking at Canada’s exports closely to determine if they will also need to be blacklisted.
Natural News reported that public school educators in Minnesota, including schools in Hopkins, Orono, Shakopee, Westomka, and Minneapolis have announced that they will gradually phase out GMOs (genetically-modified organisms) from their meal offerings as part of a long-term effort to teach students about proper nutrition and the dangers of biotechnology.

The Organic Consumers Association reported that Stonyfield Farm has resigned from the International Dairy Foods Association (IDFA). IDFA is a trade group that is suing Vermont to overturn the state’s GMO labeling law, passed earlier this year.

Sustainable Pulse reported that the Mexican Chapter of the Permanent Peoples’ Tribunal has called on the Mexican government to ban the planting of genetically modified (GM) maize in the country. The decision cited the importance of maize as one of three principal staple crops globally, which millions depend on. The Tribunal, which considered evidence gathered over three years from over 1000 organizations on this and other issues, also highlighted the importance of Mexico as the centre of origin of maize globally.

The Global GMO Free Coalition reported that the International Federation of Organic Agriculture Movements (IFOAM) has joined the Global GMO Free Coalition (GGFC) in a move that has added to the pressure currently being applied on the Biotech industry worldwide. IFOAM along with other partners works to fight for the protection of pesticide-free agriculture in Asia and Africa.

Food Production Daily reported that an ammonia leak at a Tyson Foods plant in Rogers, Arkansas caused 25 employees to seek medical attention at local hospitals and 250 people to be temporarily evacuated from the plant.

British dairy farmers are suffering as milk prices continue to plunge, reports Farmers Weekly, one of Great Britain’s leading agricultural publications. Last week, Dairy Crest, First Milk and several smaller processors issued price cuts of more than 1p/litre, following Arla’s latest drop last Tuesday, the publication reports.

On Thursday, December 11, 2014 dairy farmers drowned politicians’ portraits in milk in a protest against plunging prices. More than 350 farmers from 10 countries joined the European Milk Board’s demonstration outside the offices of the EU Commission in Brussels. Farmers filled a lake of milk containing pictures of European leaders like German chancellor Angela Merkel, French president François Hollande and EU farm commissioner Phil Hogan. They then set fire to straw bales in the middle of the street.

Insurance/Healthcare

Thanks to new amendments to the Canadian Health Information Protection Act (HIPA), people’s health privacy has been strengthened. The amendments include offenses for “snooping,” willful disclosure of personal information, and not properly securing health records. The changes also provide a system that will enable quick response to discovery of abandoned or unsecured records.

A recent Federal Trade Commission settlement with a medical billing company shines a spotlight on deceptive practices related to the collection and disclosure of patient’s personal health information. The case illustrates why healthcare providers must assess authorizations carefully before releasing patient health data to third parties, especially as the exchange of electronic health information between disparate organizations becomes more widespread. And it spotlights the need for Web portal providers and others to explain clearly to consumers what data they collect and what they will do with that information.

Drugmakers and Internet companies are quietly joining forces to link U.S. pharmacy records with online accounts to target ads to people based on their health conditions and
the prescription drugs they buy. In a little-known process, third-party companies assign patients unique numerical codes based on their prescription-drug records, a practice websites also rely on to track their registered users. The two sets of data can be linked without names ever changing hands, allowing pharmaceutical companies to identify groups that use a specific medicine and send them tailored Web ads.

- Federal regulators are sending a powerful message about the importance of applying software patches by slapping an Alaska mental health services providers with a $150,000 HIPAA sanction. The Department of Health and Human Services’ Office for Civil Rights says Anchorage Community Mental Health Services’ failure to apply software patches contributed to a 2012 malware-related breach affecting more than 2,700 individuals

- Federal regulators have issued a strategic health IT plan for 2015 to 2020 that includes five major goals, including advancing secure health information exchange.

- The National Health Information Sharing & Analysis Center is making available for free to its members a new intelligence platform that aims to help ease cyberthreat information sharing. The introduction of the new NH-ISAC Threat Intelligence Platform comes as another healthcare industry organization, the Health Information Trust Alliance, is also gearing up to release a previously announced cyber-alert system for the sector in January.

- A new report, dated September 29, 2014 but released on December 2, 2014 by the Treasury Inspector General for Tax Administration, says improvements are needed to ensure the security of information provided to the IRS by health insurers and pharmaceutical manufacturers for the Affordable Care Act program.

---

**Financial**

**Financial Services**

**Activism**

- Occupy Wall Street conducted an anti-police brutality protest against the current New York City police commissioner at a lunch event organized by a local chamber of commerce in NYC on December 10, 2014.

- A protest against “inequality and systemic racism” will occur December 15, 2014 in Seattle, WA. Participants are encouraged to go “all out in the streets.”

- A housing activist group will travel to Washington, DC on January 8, 2014 to confront the Director of the Federal Housing Finance Agency about housing injustices. The group said supporters should look out for actions in December, leading up to the meeting in Washington, DC.

- A UK-based activist group that campaigns on issues of global justice and development in the Global South hosted “carol singing in praise of TTIP” in Central London, UK on December 9th. Activists met in front of the Department for Business, Innovation, and Skills and proceeded to Trafalgar Square for an anti-TTIP rally.

- Pro-democracy activists held a protest last week in London, UK against the Ukrainian Investment Summit that was held in the city from December 9-10, 2014.

- In solidarity with several anti-government hunger strikers in Greece, an undisclosed anarchist group posted an announcement, claiming responsibility for targeting ATMs of leading Greek banks in several cities and issued a threat of more vandalism if their demands are not met.
• Chicago Anonymous conducted a ‘Millions March Chicago’ event on December 13, 2014 in Chicago, IL. The event was held in solidarity with the ‘Millions March NYC’ event in NYC that occurred the same day. The events demanded justice for Michael Brown and Eric Garner.

• Housing activists will conduct an eviction defense action in Plymouth Township, MI on December 16, 2014 in support of a local homeowner facing eviction.

• Employees of a janitorial and building maintenance organization serving the San Francisco Bay Area will conduct a picket on December 18, 2014 in the San Francisco Financial District. Participants will call for higher wages, and speak out against unsafe working conditions and sexual harassment.

• Occupy Wall Street will conduct a police brutality protest action on December 19, 2014 at City Hall in NYC. Event organizers have also called to boycott a leading area media organization for its “continued bias, racist untruths and misrepresentation” regarding police brutality cases in NYC. A counter-protest organized by an NYPD supporting group will also occur at City Hall on the same day and time.

• Occupy Wall Street will conduct a Martin Luther King Jr. action on January 19, 2015 in New York City. Considering the ongoing police brutality events occurring nationwide, it’s likely this Dr. King Jr action on January 19, 2015 will escalate into a large participant turnout with area disruptions.

**Information Security Risk**

• Researchers said that by the end of 2014 the technology industry will see the biggest increase in the number of software vulnerabilities in at least the past five years. A new vulnerability update report covering August-October 2014 predicted that by the end of the year the industry would see an increase from 2013 of around 40% in discovered vulnerabilities.

• Cybercriminals are using a new variant of the Neverquest malware to target the customers of financial institutions worldwide. The banking Trojan was first spotted in November 2013, and the threat is believed to be an evolution of the Snifula malware family. New variants of Neverquest were released this summer with most infections spotted in the United States and Japan.

• Cybercriminals are using an “extremely” stealthy trojan called Turla to siphon sensitive data from governments and pharmaceutical companies around the world. For at least four years, the campaign is said to have targeted government institutions, embassies, military, education, research, and pharmaceutical companies in more than 45 countries. The yet-to-be identified attackers are believed to be backed by a nation-state and are known to have infected several hundred Windows-based computers by exploiting a variety of vulnerabilities, at least two of which were zero-day bugs.

• The U.S. Treasury Department found that a majority of bank account takeovers by cyber thieves over the past decade might have been thwarted had affected institutions known to look for and block transactions coming through Tor, a global communications network that helps users maintain anonymity by obfuscating their true location online. In the report, released on December 2, 2014, FinCEN (Financial Crimes Enforcement Network) said it examined some 6,048 suspicious activity reports (SARs) filed by banks between August 2001 and July 2014, searching the reports for those involving one of more than 6,000 known Tor network nodes. Investigators found 975 hits corresponding to reports totaling nearly $24 million in likely fraudulent activity.

• A new self-replicating ransomeware dubbed W32/VirRnsm-A infects nearly anything throughout the user’s network, resists being removed, and spreads like a virus. The malware can spread by normal means, such as by opening an infected email or by going to a malware-infected Website. Once the malware is downloaded, it begins operation by infecting data files, which could be anything from PDF files to JPG photo files. From a
single computer, the infection can spread on its own throughout a corporate network.

- A new survey concludes that 71% of respondents said they have access to data they should not see, and more than half said that this access is frequent or very frequent. The findings of this survey are derived from interviews conducted in October 2014 with 2,276 employees in the US, UK, France, and Germany. Respondents included 1,166 IT practitioners and 1,110 end users in organizations ranging in size from dozens to tens of thousands of employees, in a variety of industries including financial services, public sector, health & pharmaceutical, retail, industrial, and technology and software. Other highlights include: 4 in 5 IT practitioners say their organizations don't enforce a strict least-privilege (or need-to-know) data model; Only 22% of employees say their organization is able to tell them what happened to lost data, files or emails.

- Researchers discovered a new PoS malware family, which they named “LusyPOS” after a Russian underground forum where it was first observed. The malware shares similarities with the Dexter family of PoS malware, but, unlike Dexter, it’s known to use the Tor network to connect to its command-and-control (C&C) servers.

- Hackers claimed to have hacked a major U.S. credit card company, along with a host of several American universities and a French airline company.

- A payment solutions provider began warning merchants and cardholders of a data breach that may have exposed information related to payment card transactions dating back as far as November 5, 2009. The New Jersey-based company, whose solutions route payment transactions from merchants' point-of-sale systems to their payment processors, discovered malware on its systems on September 22, 2014 that had not been previously detected by any anti-virus program.

- The Better Business Bureau (BBB) warned of a high-tech check-cashing scam, which uses mobile banking apps to trick account holders into sharing their bank information. The BBB said that scammers are using a multi-pronged approach involving social engineering and legitimate mobile banking apps to leave victims holding the bag when it comes to purloined funds.

- A new wave of highly sophisticated cyberattacks dubbed ‘Inception’ is targeting embassies, military installations and major corporations around the world. Researchers describe Inception as a "very slick operation" that points to a "very high chance of state involvement." Characteristics of Inception include randomized file names to prevent detection, cloud encryption and malware components embedded in Rich Text Format (RTF) files. Documents associated are in Hindi, Russian, Swedish and English, while one piece of code carries the line "God Save the Queen," though any of these could be red herring devices.

- A new study said Chinese internet users are behind 85% of fake websites. Of the 22,679 malicious domain registrations that the study reviewed, over 19,000 were registered to servers based in China. This is in addition to nearly 60,000 websites that were hacked in the first half of 2014 and then used to acquire people's details and credit card information while pretending to offer real goods or services.

- Researchers announced a new SSL/TLS problem on December 8, 2014 and said it's likely to affect some of the most popular web sites, including those belonging to banks, investment firms and credit providers. The vast impact is due largely to the popularity of certain load balancers manufactured by an American IT company specializing in Application Delivery Networking (ADN) technology. There are also other devices known to be affected, and it's possible that the same flaw is present in some SSL/TLS stacks.

- The exploit known as POODLE attack (which stands for "Padding Oracle On Downgraded Legacy Encryption") is a man-in-the-middle exploit which takes advantage of Internet and security software clients' fallback to SSL 3.0. If attackers successfully exploit this vulnerability, on average, they only need to make 256 SSL 3.0 requests to reveal one byte of encrypted messages.
**Legal, Litigation, Regulatory Risk**

- An article reported that the Securities and Exchange Commission is making an effort to make the cost of compliance violations steeper by refusing to give companies “a free pass.” As part of the settlement with a leading U.S. bank, the S.E.C. has filed charges of securities fraud that required the bank to admit that it “engaged in fraudulent conduct.” The article highlighted that the bank will need to prove good cause to obtain a waiver from the “bad actor exclusion” under Rule 506 after its mortgage-backed security settlement.

- A leading U.S bank has agreed to a second state settlement tied to a data breach involving the loss of two backup tapes that may have exposed personally identifiable information for 260,000 of the bank's 8 million U.S. customers. The $625,000 settlement with the Massachusetts attorney general is separate from an earlier, $850,000, nine-state settlement. Massachusetts pursued its own investigation because the breach occurred in that state and affected a large number of its residents. In the Massachusetts settlement, Attorney General said the breach exposed the personal information of more than 90,000 Massachusetts customers.

- An article reported that a leading U.S. bank is currently fighting a case filed by a consumer that received a 1099-C form from the bank. Although the bank dodged federal claims — notably FDCPA — in the case, it will still have to defend other charges in state court. The article advises that any debt firm that sends 1099-C forms to consumers should watch developments closely. In 2010, the bank began internal debt collection efforts against a consumer for two overdue credit card accounts. The consumer claimed that he never had a credit card with the bank and insisted that the accounts were not his. He hired an attorney who directed the bank to send all communications to their legal office. But the bank continued to contact the consumer threatening legal action and referral to a collection agency. In January of this year, the bank sent a 1099-C form to the consumer informing him that the bank had reported nearly $7,500 in debt forgiveness to both the IRS and his state’s (Alabama) revenue department in closing the accounts. When the consumer’s lawyer contacted the bank, it referred him to the bank’s fraud department. The consumer sued the bank in April alleging violations of the FDCPA and a host of state laws including negligence, private nuisance, and wantonness. The case was originally filed in state court, but the bank moved it to federal district court to answer the FDCPA claim.

- An article reported that “liberal members of Congress” have expressed reservations about the $1.101 trillion bill to fund the government through September as these provisions would change the way government regulates big banks.

- An article reported that Congress has agreed to use the FDIC to “cover” risky trading by the nation's biggest banks. The article highlighted that the budget bill repeals a portion of the Dodd-Frank financial reform act and lays the groundwork for future bailout of banks that make irresponsibly risky trades. The head of a financial watchdog group remarked that if Wall Street gets the “upside in big bonuses” from its high risk deals, then it should also have to pay the “downside for any losses.”

- An article reported that a former computer technician for a leading U.K. financial institution was indicted in Switzerland on charges of industrial espionage and violating the country's bank secrecy laws, prosecutors said. The Swiss Attorney General’s office, without identifying the suspect as is its custom, said in a statement that the country was prepared to try him in absentia. The statement refers to the technician accused of stealing client data in 2008 from a Geneva office of a leading U.K. bank and passing it to French authorities.

**Operational Risk**

- The two GSEs for housing on December 8, 2014, released the final guidelines for low down payment mortgage loans, reviving a practice that critics say could eventually lead
to defaults and another financial crisis. Industry experts said the new loans could eventually inject more risk into the housing market, and taxpayers will again foot the bill if the GSEs’ mortgage loans default in large numbers.

- An article reported that banking regulations in Cayman don’t require banks to tell customers if their data has been compromised by hackers, and that is the same for all industries in Cayman. However, new data protection legislation, which has been circulating in the Legislative Assembly for years, would add consumer protections and could potentially force banks to share information with customers when data is stolen.

**Reputational Risk**

- Environmental activist groups sent letters to 26 banks to express their concerns regarding several global pulp and paper companies and their sister companies due to their involvement in large scale deforestation and social conflicts. In the letter, the activist groups request assurances that banks are not currently investing in any of these companies, and that they will not do so until they end their illegal and unsustainable environmental and social practices and achieve a performance consistent with the EPN Performance Milestones.

- A German activist group campaigning against corruption and use of illegal weapons published its report 'Dirty Profits 3 - Report on Companies and Financial Institutions Benefiting from Violations of Human Rights' that exposes financial relationships between selected major European financial institutions and multinational companies, across various sectors, that have consistently violated environmental and human rights standards.

- An article reported that many leading U.S. banks conducted foreclosures against active-duty service members.

**Global Intelligence**

**China**

- Continued labor strikes in Southeastern China, particularly in the Shenzhen region.

- Chinese news outlets reported that Taiwan-based Wanshida in Dongguan will be ceasing operations, which will impact 7000 employees. On December 5, 2014 it was announced that due to restructuring plans, Wanshida’s parent company, Shenghua Group would be closing two of its Dongguan businesses. After the announcement, it was reported that local government offices and organizations have already stepped forward with plans to enroll displaced workers into reemployment programs.

- The All-China Federation of Trade Unions reported various measures taken by the Yiwu Trade Union Federations (Yiwu, Zhejiang) to prevent the recurrence of wage disputes. In summary, the federation provided legal services, monitored the operations, built sound wage payment security systems, and enhanced inspection and supervision of companies in the city.

- Sina Tech News reports that over 2000 workers went on strike at Suzhou Lianjian Technology factory on Dec 9, 2014, causing damage to company equipment inside and outside the plant. Workers were dissatisfied with severance compensation amounts after the plant's closure was announced on December 5, 2014. Lianjian Technology is a Taiwanese-owned subsidiary which produces LCD display components for global companies such as Apple and Xiaomi.

- Radio Free Asia reported that over a thousand workers went on strike at Shenzhen Qingsheng Clothing and Accessories Limited Company, due to social insurance and housing fund benefits still owed to workers by the company. Workers protested outside
the factory, demanding the funds be paid in full.

- A Chinese technology news outlet reports recursive DNS in multiple provinces in China experienced DDoS attacks and caused nationwide DNS instability.

- A Chinese news outlet reports 67 malicious application being taken down from multiple Chinese application stores. According to the article, Baidu is among one of the application stores.

- A Chinese news outlet reports 1.5 million Wi-Fi passwords have been stolen from a Shanghai company that develop Wi-Fi Hotspot Application. According to the article, the hackers exploited Wi-Fi sharing applications to remotely control by injecting malicious codes to these applications and turned users devices to bots.

- A Chinese cyber security news outlet reports AliExpress website contains a security vulnerability that could be exploited by hackers and change sellers’ merchandise prices.

**Germany**

- The German Federal Criminal Police Office and the Max Planck Institute for Foreign and International Criminal Law published a study based on a survey of 35,000 individuals regarding experiences of being victimized by criminals, sense of security, and attitudes towards crime-related issues (German Victimization Survey 2012). The study is meant to supplement the official Police Criminal Statistic, which only describes officially registered cases.

**India**

- The Times of India reported that the employees union and management will meet the assistant commissioner of labor on Friday to officially start the process of fixing the severance package for 1,700 workers who will be displaced when Foxconn suspends production on December 24, 2014. Foxconn is stopping production at its Sriperumbudur plant in the Nokia SEZ due to lack of orders after its biggest customer in India, Nokia, exited the cellphone business.

**Israel**

- On December 8, 2014 IndustriALL reported that Israeli union federation Histadrut has succeeded in increasing the minimum wage for private workers in Israel by 700 ($175 USD) rather than NIS 200 ($50 USD) proposed by the finance minister.

**North America**

- On December 11, 2014 The Daily Beast reported that the Supreme Court ruled in a 9-0 decision that Integrity Staffing Solution, a subcontracted company where workers process and ship Amazon goods, does not have to pay its workers for the time that workers have to submit to screenings. Integrity Staffing Solutions employees have to undergo screenings at the end of the day, every day, to ensure they aren't stealing from the company.

- Oregon Live reported that the Port of Portland Commission on December 10, 2014 authorized a purchase of more than 46 acres of vacant land for nearly $9.9 million from SolarWorld. SolarWorld recently announced a $10 million expansion of its plant, and the company said it would add 200 jobs in Hillsboro as it tries to meet increasing demand for solar panels in America.

- USA Today reported that Apple and Amazon are refusing to release federal data on the diversity of their workforces. The article noted that Facebook, eBay, Google, Yahoo, and LinkedIn are among the technology companies that have made public their EEO-1s.

**Vietnam**

- Info.VN, a local VNese media source, reported that hundreds of people have set up
tents and barricades in front of the gate of the Vietnam-France Steel Factory to protest the company's discharge of harmful smoke in the environment. For a long time, the factory has discharged smoke and dust both day and night, affecting the health of people. Although local people had reported the problem to the authorities several times, environmental pollution has not been solved. This company has recently operated at its full capacity so the pollution has become serious. According to people, no matter whether it is day or night, though the doors are closed, smoke still storms into houses, making it hard to breathe. Because of the encirclement, scrap trucks could not enter the factory for the past several days so the plant's nearly 300 workers had to cease production. The protest took place 533 miles from Intel in Ho Chi Minh City, Vietnam.

Legal and Regulations

- On December 10, 2014, the New York Department of Financial Services (NYDFS) issued a letter to banking institutions chartered or licensed in New York notifying them of an expansion of the NYDFS information technology examination procedures to focus on cyber security issues as an integral aspect of risk management. The expanded procedures will look at cyber security in a comprehensive manner and will include a review of corporate governance as it relates to cyber security risks, the relationship between information security and core business functions, shared infrastructure risks, training, disaster planning and insurance coverage and other third-party protection.

- A recent California case, shows that even a properly formed online contract may be unenforceable if its terms are overly harsh and one-sided. Given that website terms are routinely drafted to be favorable to the website operator rather than the user, this case serves as a reminder that contract formation is not the only issue that must be considered when discussing the enforceability of online contracts. The case, MacKinnon v. IMVU, Inc., was brought as a putative class action by plaintiff Peter MacKinnon, a user of defendant IMVU's instant messaging virtual universe. There is still more to come from this case but given that website terms often include provisions that are seemingly no more “harsh,” “oppressive” or “one-sided” than was the IMVU no-refund provision, website operators may wish to review their existing terms in light of the MacKinnon case. In particular, MacKinnon suggests that unilateral amendments of website terms that impact users’ previous purchases without adequate compensation may be suspect.

Pharmaceuticals

- Drug makers and Internet companies are quietly working together to link U.S. pharmacy records with online accounts in order to target ads to people based on their health conditions and their prescription drugs, Bloomberg News writes. In a little-known process, third-party companies assign patients unique numerical codes based on prescription records, a practice websites also rely on to track their registered users, the news service writes. The data sets, Bloomberg explains, can be linked without names changing hands, allowing drug makers to identify who uses a specific medicine and to send customized Internet ads. The practice has become an essential part of digital marketing efforts by drug makers, according to Bloomberg. But while the industry says the technique complies with federal medical privacy laws because patient names are concealed, critics see a breach of confidentiality.

- Online medical bill site PaymentsMD tricks people to handing over health records. The PaymentsMD have allegedly misled thousands of consumers who signed for the billing portal, by failing to adequately inform them that the company would seek highlight detailed medical information from pharmacies, medical labs, and insurance companies.

- AstraZeneca next year plans to close a manufacturing plant in Massachusetts that made...
the Pulmicort asthma treatment, costing 180 employees their jobs

- Several EU member countries have suspended marketing authorization for therapies that underwent bioequivalence testing at contract research organization GVK Biosciences’ facility in Hyderabad, India over serious concerns with good clinical practice.

Retail

- Earlier this month, security researchers discovered a new PoS malware family, which they named “LusyPOS” after a reference in Russian underground forums. We detect this as TSPY_POSLUSY.A. In their analysis, they mentioned that it had some characteristics linked to the Dexter family of PoS malware. It also had behavior similar to the Chewbacca PoS malware (which we detect as TSPY_FYSNA.A), which is known to use the Tor network to connect to its command-and-control (C&C) servers.

- Electronic payment gateway solutions provider CHARGE Anywhere, LLC said on Tuesday that an attack against its network resulted in hackers gaining access to payment card data for transactions processed through many merchants. The hackers breached the systems and had the ability to capture data as early as November 5, 2009. CHARGE Anywhere said, using malware that had not been previously detected by any anti-virus program.

- The Asprox botnet was responsible for about 80 per cent of all attack sessions recorded during October 2014, impacting nearly 2,000 different organizations. These figures, from a new report by Palo Alto Networks, provide evidence that the Asprox (AKA Kulooz) malware family is continuing to plague businesses, despite multiple attempts to disrupt its infrastructure. The Asprox botnet, which first surfaced around six years ago in 2008, has been linked to phishing scam messages as well as the distribution of secondary malware infections. The zombie network also acts as a platform for hack attacks. Retail and wholesale organizations received almost 28 per cent of malware over the web channel while hospitality firms received less than two per cent of badness via web channels.

- Online sales at third party marketplaces grew faster than the overall industry, according to cloud-based e-commerce solutions provider ChannelAdvisor. However, malls remain the most important shopping venue for millennials aged 16 to 26.

- Teen retailer Wet Seal may file for bankruptcy protection if it fails to resolve its liquidity issues.

- Facebook is working on a number of methods, "Custom Audiences" among them, designed to give retailers a way to gauge how the platform's advertising affects in-store purchase behavior.

Technology

- The AnonGhost hackers are active once again, the Mauritania Attacker seems to be one of the pull horses which is pulling the AnonGhost towards aggressive hacking. This time the AnonGhost hackers claim that they have hacked the Israeli Mozilla Firefox environment.

- A Chinese news outlet reports Sony Picture employees received threatening emails demanding the employees to sign an attachment included in the email against Sony Picture.
A Chinese cyber security news outlet reports a new POS malware, LusyPOS has surfaced and is being sold in underground market at starting price of $2,000.

A Chinese news outlet reports a trojan malware dubbed as "Mad Cow" preying on investors by spreading via stock transaction applications in order to steal fund through online bill pay.

A Chinese news outlet reports POS malware surfaced in Japan for the first time.

A Chinese cyber security news outlet contains information regarding a malicious trojan, FakeDebuggerd. The trojan are able to gain root permission and install files on Android system.

Palo Alto Networks unveiled a new analysis of malware trends affecting thousands of organizations and major industries. Among the findings, which were released today as part of the new Unit 42 Threat Landscape Review, is the persistence of the Kuluoz or Asprox malware family, which accounted for a majority of malware attack sessions affecting industries as varied as healthcare, retail and financial services.

A growing number of flaws in web browsers is viewed as the biggest endpoint security headache by today’s IT decision-makers, according to Malwarebytes. With the number of exploitable browser vulnerabilities accelerating this year, 72% of the 685 IT decision-makers questioned said this made security difficult in their organization, more so than any other issue.

German union Verdi has called for a three-day strike at five Amazon distribution centers in Bad Hersfeld, Leipzig, Graben, Rheinberg and Werne as a result of a long dispute over pay. The walkouts are to start from Sunday night December 14, 2014 and will run until the end of Wednesday’s late shift.

Germany, which is spearheading Europe’s fight against U.S. tech giants on everything from data privacy to Google’s search engine monopoly, is hoping to scupper net neutrality too. Behind the push: hoping that faster, cloud-based services will boost German manufacturing.

Hackers are threatening to release more sensitive data from last month’s massive cyber break-in. "We are preparing for you a Christmas gift," the group posted on a website. "The gift will be larger quantities of data. And it will be more interesting. The gift will surely give you much more pleasure and put Sony Pictures into the worst state."

Microsoft is preparing to fight a U.S. government search warrant that seeks its customer emails stored abroad.

Telecommunications

What difference does a month make? In telecom, the answer is about $45 billion. That’s how much market value Verizon Communications Inc., AT&T Inc., Sprint Corp. and T-Mobile US Inc. have lost collectively since mid-November amid a fast-moving reassessment of the industry’s value by investors. The lost value is greater than the current market capitalization of Sprint and T-Mobile combined.

Where the U.S. eventually lands on the issue of net neutrality could have wider reaching international implications, including the possibility of opposition from the U.N. and World Trade Organization (WTO).

Entertainment
Fallout from the Sony hack has continued after reports that sensitive contracts, unpublished scripts and salaries of top executives were leaked online. A recent email paper chain between two high-level executives disclosed an internal battle regarding the movies “Jobs” and the in development Angelina Jolie film “Cleopatra.” This is just the latest of what may be many devastating leaks following the recent data breach on Sony.

Defense

- A sophisticated cyber-espionage campaign believed to be the continuation of the Red October operation has been identified to target specific users of Android, iOS and BlackBerry mobile devices through spear-phishing attacks. Researchers from provider of security and network solutions Blue Coat have uncovered the endeavor that leverages a complex infrastructure relying on “a convoluted network of router proxies and rented hosts, most likely compromised because of poor configurations or default credentials,” to deliver targeted malicious emails. In an extensive report on Inception/Cloud Atlas, Blue Coat revealed that the threat actor planned attacks on mobile devices of high-profile targets in different sectors, from finance and oil industry to military, engineering and politics, in different parts of the world.

- The United States Department of Justice has created a unit solely focused on tackling cyber crime and concerns about privacy in criminal investigations arising from Snowden revelations.

- ISIS uses control of natural resources, namely water as a tool of war. ISIS has established a blueprint that can be used by other entities to take advantage of drought and water scarcity.

- Five international aviation organizations have signed a new cybersecurity agreement to focus their respective actions on cyber threats against the global aviation system. The International Civil Aviation Organization (ICAO), Airports Council International (ACI), Civil Air Navigation Services Organisation (CANSO), International Air Transport Association (IATA) and International Coordinating Council of Aerospace Industry Associations (ICCAIA), formalized a common front against hackers, hacktivists, cyber criminals and terrorists who pose potential cyber threats ranging from theft of information and general disruption to potential loss of life.

- The Defense Advanced Research Projects Agency (DARPA) is trying to get ahead of most persistent threats (APTs) in cyberspace and is putting up $60 million to find innovative ideas. The research agency posted a request for proposals for a Transparent Computing program designed to shine a light on malware hiding in the depths of complex computer systems and actively adapt to new threats.

- Cyber espionage attacks are expected to increase in 2015 with an emerging field called “cybercrime-as-a-Service” will become more prevalent. Mobile attacks will continue to proliferate with more deployment of malware generation kids and malware source code. The vulnerabilities in the Internet of Things will be exploited.

Law Enforcement

- After four straight nights of anti-police protesters crowding San Francisco Bay Area streets — prompting authorities to fire rubber bullets at crowds and arrest 19 people late Tuesday alone — the hacker collective Anonymous on Wednesday apparently sought vengeance. Several websites for the city of Oakland were knocked out in a likely cyberattack. By Wednesday night, the sites for the city and the Fire Department were operating, but the
Police Department's website remained disabled. In a message posted on Anonymous' main Twitter account, the group took responsibility by posting "Tango down: oaklandpolice.com."

- With widely watched amateur videos of police killings as a backdrop, New York City police are hoping to arm more officers with stun guns as an option for subduing emotionally disturbed people and other suspects who resist arrest. Preliminary plans call for 450 additional officers to carry the electroshock weapons while on patrol, police officials said. The department would first have to find funding and develop more precise guidelines on which circumstance are appropriate to use the devices.

- Swedish police have raided a server room in Stockholm in an action targeting the file-sharing website The Pirate Bay. Police spokesman Paul Pinder said Wednesday the raid took place after Rights Alliance, a Swedish Internet anti-piracy group, had reported Pirate Bay for alleged copyright violations. He declined to give further details. He said the file-sharing website went down shortly after Tuesday's raid.

- U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) has teamed with industry and 24 law enforcement agencies across 18 countries to shutdown 29,684 domain names that were illegally selling counterfeit merchandise online as part of Project Transatlantic/Operation In-Our-Sites V.