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

Get Your Free Trial for the Cyveillance Cyber Threat Center

The first cloud-based intelligence platform designed specifically for security, cyber, and threat analysts

The Cyber Threat Center is an easy-to-use platform that helps you better protect your organization with the richest and deepest collection of online threat intelligence available anywhere, and a powerful suite of tools.

Put the power of Open Source threat intelligence (OSINT) to work for your organization today!

---

Top Incidents

**Energy**

- The Environmental Integrity Project released a new report critical of the so-called "Halliburton Loophole" that exempts fracking fluids from the Clean Air Act, Clean Water Act, Safe Drinking Water Act, and CERCLA.

**Agribusiness**
A recent audit by the Office of the Inspector General revealed that the Food and Drug Administration’s computer network is vulnerable to a potential data breach. The news is especially critical as almost exactly one year ago it was discovered that the FDA’s online submission system was breached by an unauthorized user.

**Insurance/Healthcare**

- In the last five years, the number of data breaches in the medical sector has quadrupled. Last year, for the first time, the medical sector experienced more breaches than any other. It’s again on track to lead in 2014 – so what is behind the dramatic rise in medical identity theft? A decentralized U.S. health system, increasing digitization of records, and demand in the black market are fueling a surge in thefts.

**Financial Services**

- Pro-Islamic hackers penetrated a stock exchange in Warsaw, Poland last week and gained “unauthorized” access to some archival log in data. Sources said the attack started on the server utp.gpw.pl from where the attack escalated and lasted for several days. The hackers declared in a series of posts published on a popular data dump site that all the governments that joined the bombing of the Islamic State are now their targets, specifically suggesting that Europe’s "peaceful life is over." Further, the posts warned that “Your money, your information and your lives are under our control.”

**Global Intelligence**

- Epoch Times reported that over a hundred workers went on strike at Shuangye Metal Products Limited Company in Dongguan from Oct 20-22. Workers protested due to docked overtime pay and social welfare benefits in arrears. The incident resulted in a violent confrontation with police, causing 8 to be arrested and 4 to be injured.

**Legal and Regulations**

- A new class action lawsuit alleges that on LinkedIn “any potential employer can anonymously dig into the employment history of any LinkedIn member, and make hiring and firing decisions based upon the information they gather, without the knowledge of the member, and without any safeguards in place as to the accuracy of the information that the potential employer has obtained.” The case is *Tracee Sweet et al v. LinkedIn* which was filed on October 4, 2014 in the US District Court for the Northern District of California.

**Pharmaceuticals**

- One of the biggest attack campaigns against critical infrastructure since Stuxnet might not actually have been aimed at critical infrastructure. New research on the Dragonfly, a.k.a. Energetic Bear, attacks that were first reported by F-Secure in June poses the theory that the group's true target was the pharmaceutical and biotechnology industry, not the energy sector. In a report released today by the signal transmission solution company Belden, Joel Langill, an industrial control systems security expert at RedHat Cyber, explains why he thinks Dragonfly was attacking small companies that supply original equipment manufacturers, which in turn supply the pharma-biotech sector.

**Retail**

- Staples is looking into a potential credit card data breach and has been in touch with law enforcement officials about the issue. The office supplies retailer said Tuesday that if it turns up any data discrepancies during its investigation, customers won’t be responsible for fraudulent activity on their credit cards as long as it is reported in a timely manner.

**Technology**

- A Chinese web monitoring group published a report saying Apple users in China have been targeted in a sophisticated and widespread attack by hackers seeking private
user data stored on the iCloud service.

**Telecommunications**

- Fraud scams targeting the customers of several large American technology companies are seeking to provide password recovery and technical support to consumers for a weekly fee. These services, which target customers of Yahoo!, Google, Cisco, Apple to name a few, are otherwise offered for no charge by the company.

**Entertainment**

- A new partnership by Nielsen and Adobe intends to fix some TV rating system limitations. A new system will allow the audiences to be measured across every device with an IP address which will dramatically expand the number of platforms that Nielsen’s ratings can incorporate. The system will cover online content in addition to traditional video content.

**Defense**

- Trend Micro researchers identified a cyberespionage operation dubbed “Operation Pawn Storm” that uses targeted emails and compromised Web sites to infect users in government, military, and media organizations with the SEDNIT (also known as Sofacy) malware.

**Law Enforcement**

- The Justice Department accused some Ferguson officials of leaking information to the media in an effort to support Officer Darren Wilson. In recent days, details of the investigation have appeared in local and national news coverage at a time when a grand jury decision is imminent on whether Wilson will be charged in the killing of an unarmed black teenager.

**Energy**

- Greenpeace New Zealand is pushing to have Shell fined for drilling two offshore wells without appropriate permits.

- An activist petition indicates a belief that hydraulic fracturing activities pose risks to the Squaw Creek Comanche Park nuclear plant.

- The Environmental Integrity Project released a new report critical of the so-called “Halliburton Loophole” that exempts fracking fluids from the Clean Air Act, Clean Water Act, Safe Drinking Water Act, and CERCLA.

- The group FracTracker is organizing volunteers to monitor oil trains and count cars in order to track shipments of unconventional oil. The group has posted at least one video of these activities so far.

- A formal complaint was filed with the International Criminal Court in the Hague against Chevron for their refusal to clean up the toxic contamination of Ecuador’s Amazon Rainforest. The complaint states that their actions constitute an “attack” on civilian population impacting indigenous and farming communities. The petition charges that the systemic harm inflicted by Chevron constitutes a “crime against humanity” and therefore is of concern to the international community. “It is critical that all legal mechanisms be fully utilized to put an end to what is effectively impunity for a major American oil company that is committing human rights crimes against vulnerable populations,” said Pablo Fajardo, lead lawyer for the impacted communities.

- Rising Tide Vermont is promoting a rally and sit-in on the Montpelier Statehouse Lawn on October 27 and highlighting the past 6 months of organizing and direct action against the Fracked Gas Pipeline! The rally will call on the Shumlin Administration to
stop the fracked gas pipeline and protect Vermonters’ (and everyone’s) right to a healthy environment and livable planet.

- The London-based Carbon Disclosure Project (CDP), which serves as a vehicle for businesses to report their greenhouse gas emissions, has issued its first-ever Climate Performance Leadership Index, revealing its “A List” of corporate citizens who are doing the most to respond to climate change. One of the bold actions taken by CDP is to name TransCanada—the company behind the Keystone XL pipeline—a “global climate performance leader.” While TransCanada has investments in solar, wind and hydro power, it’s best known for the unfavorable attention it has attracted over the past six years for its proposal to build the Keystone XL pipeline to ship tar sands oil from Alberta to the Gulf of Mexico.

- Texas’ chief toxicologist is arguing that the EPA shouldn’t tighten ground-level ozone, or smog, rules because there will be little to no public health benefit. Dr. Michael Honeycutt heads the toxicology division of the Texas Commission on Environmental Quality (TCEQ), the state agency tasked with protecting Texans from pollution. “Ozone is an outdoor air pollutant because systems such as air conditioning remove it from indoor air,” he argues on a blog post on the TCEQ website. “Since most people spend more than 90 percent of their time indoors, we are rarely exposed to significant levels of ozone.” He adds that those who are “near death” and thus more vulnerable to ozone spend even more time inside.

- A host of chemical emissions seep are seeping from oil and gas drilling pads with different ones coming from different places in the operation – from the wellhead to tanks to valves, according to a new study. The study is one of several being done in Utah’s Uintah Basin, which has been the scene of winter ozone levels that exceeded readings in New York City. The eastern Utah basin is home to more than 10,000 oil and gas wells, with 1,000 wells being added every year. The research was conducted by scientists at the Cooperative Institute for Research in Environmental Sciences at the University of Colorado-Boulder and the National Oceanic and Atmospheric Administration. What the researchers found was that methane – a potent greenhouse gas – came primarily from the wellhead as did methanol.

- Advocacy group Greenpeace said Wednesday it parked its protest vessel Arctic Sunrise off the Spanish coast to pressure European leaders on climate reforms. Members of the European Union kick off a two-day summit Thursday in Brussels to review their environmental policies. Leaders are set to discuss reducing emissions by 40 percent from the 1990 level, using renewable energy for 27 percent of their power needs and improving energy efficiency by 30 percent by 2030.

- Anti-fracking activists in Greater Manchester and West Sussex have been left concerned, but not surprised, by the results of a long-running Network for Police Monitoring (NetPol) investigation into a series of secretive agreements signed between their local police forces and private companies exploring the viability of fracking in their areas. These ‘Memorandums of Understanding’, uncovered through the persistent use of freedom of information (FoI) requests, appear to set out a working relationship between police covering the Barton Moss (Salford) and Balcombe (West Sussex) fracking test sites and the commercial interests engaged in the testing.

- The risks and benefits of fracking for the UK are to be examined by a “independent” task force, led by the former head of the Environment Agency, Lord Chris Smith, and funded by shale gas companies. “We will assess the existing evidence, ask for new contributions and lead a national conversation around this vitally important issue,” said Smith, who as chair of the Environment Agency oversaw key fracking regulation. “The Task Force on Shale Gas will provide impartial opinions on the impacts, good and bad, that the exploitation of shale gas will have on the UK.”
The Animal Liberation Front has taken responsibility for placing explosives in the bathrooms of the International Federation of Sudamerican Societies of Animal Laboratory Sciences conference in Buenos Aires, Argentina in September.

A recent audit by the Office of the Inspector General revealed that the Food and Drug Administration’s computer network is vulnerable to a potential data breach. The news is especially critical as almost exactly one year ago it was discovered that the FDA’s online submission system was breached by an unauthorized user.

The statewide referendum in Oregon over labeling foods containing genetically modified organisms is now the most expensive ballot question in state history, says the Salem Statesman Journal. The campaigns for and against Measure 92 raised $17.6 million, according to reports filed with the Oregon Secretary of State's office.

U.S. farmers say Big Data allows them to reduce costs and boost yields but they also worry the information could wind up in the hands of regulators or could be used by someone else to speculate in the commodity market, says the American Farm Bureau Federation.

The influential analysis group SovEcon says Russia's grain harvest could tally less than 50 million tonnes in 2015, a drop of at least 15 percent from this year, according to AgriMoney. The winter wheat crop is in poor condition, raising the risk of large losses to winterkill, and the weakening value of the ruble may make it harder for growers to buy supplies to sow wheat in the spring.

While China is taking extraordinary measures to reform and create efficiencies in its agricultural sector, it will likely remain a major importer of American-grown soybeans, corn, pork, and other products for decades to come. That was the view of participants in the Iowa Farm Bureau Federation’s study tour who recently toured parts of China to get a firsthand view of demand and supply issues in the world’s most populous country.

U.S. approval of Dow Chemical Co.’s Enlist Duo weed killer for treating genetically modified crops should be reversed because the government failed to adequately review its effects on human health, farmers and environmental groups said in a lawsuit.

An outbreak of Maize Lethal Necrosis Disease in Kenya may reduce corn production by almost a third this year as yields fall and growers abandon the grain for other crops, the Cereal Growers Association said.

Dairy farmers are threatening to ramp up protests against Iceland over the retailer’s decision to slash the price of four pints of milk to 89p. Farm lobby group Farmers For Action (FFA) held discussions with the Iceland senior management team on Monday (20 October) to try to persuade the overturn its decision.

Los Angeles City Council voted in support of the largely symbolic GMO Free Zone. The council voted 13-1 in support of writing legislation to ban the cultivation of GMO’s in the city of Los Angeles.

A petition was detected on moveon.org written by the group Moms Across America. The petition demands the removal of Gina McCarthy as head of the EPA. As of the writing of this report, 470 signatures have been collected.

A $25 million international study on GMO and pesticide safety will be launched on November 11, 2014. The study will be conducted by The Farmers Club in London, UK. The study will allegedly be the “largest and most comprehensive long-term experiment ever conducted on a GM food and its associated pesticide.”

The California Department of Food and Agriculture has published a draft plan that would allow the agency to spray pesticides anywhere in the state indefinitely into the future. The article has been trending with several environmental Facebook groups to rally support against the plan.
Insurance/Healthcare

- Fraud investigators and agency data-miners charged with curbing improper health care payments might take heart from a new Congressional Budget Office report on “program integrity” efforts in Medicare, Medicaid and the Children's Health Insurance Program. In a Monday report describing the budgetary impact of anti-fraud efforts by the Justice and Health and Human Services departments, the legislative cost-scoring agency said it has estimated that additional funding for anti-fraud activities “would yield savings that exceed the cost of carrying out those activities.”

- Conducting a security risk analysis is part of the core objectives that healthcare organizations must meet for Stage 1 and Stage 2 Meaningful Use. Security risk analysis can also help facilities remain HIPAA compliant in administrative, physical, and technical safeguards. Moreover, healthcare organizations can also discover any areas where this electronic protected health information (ePHI) could be at risk.

- The Metro Public Health Department in Nashville, Tennessee, is facing its second data breach since July 2014. Earlier this month, a file cabinet containing files on patients with HIV was accidentally sent to a Metro school rather than to a surplus warehouse. The agency was notified of the mix-up by the school on Oct. 8; the health department is examining its process of how files are handled during a move. This incident is believed to have occurred when the agency moved into a new office space.

- In the last five years, the number of data breaches in the medical sector has quadrupled. It's again on track to lead in 2014 – so what is behind the dramatic rise in medical identity theft? A decentralized U.S. health system, increasing digitization of records, and demand in the black market are fueling a surge in thefts.

- The deadline for all HIPAA business associate agreements (BAAs) to be up to date and in line with the regulations set forth by the Omnibus Rule was nearly one month ago. As of September 23, 2014, BAAs not renewed before September 23, 2013 were required to be compliant.

- Patient portals are slowly becoming more common in the healthcare industry, along with the option for patients to securely message their physicians through the portal. But, just how effective are those messages, and what do healthcare organizations need to keep in mind to ensure that patients’ information remains secure? Beth Israel Deaconess Medical Center (BIDMC) recently released the results of a study it conducted on the effectiveness of secure email messaging between physicians and their patients. According to the results, reimbursement models and physician workflow may need to adjust to accommodate message management.

- Cost and technical challenges remain central barriers to interoperability for health information exchanges (HIEs), according to the recent eHealth Initiative survey. The research also showed that regulatory policies have seemingly encouraged increased use of core HIE services, such as Direct, care summary exchange and transitions of care. The 11th annual survey on health data exchange used information from 125 identified HIEs, including 74 community-based HIOs, 25 statewide efforts and 26 healthcare delivery organizations.

- An Oregon health insurance exchange (HIE) has had 18 security breaches in the last six months, with the most recent one occurring when documents containing PHI was sent to the wrong patient.
More healthcare organizations might implement the National Institute of Standards and Technology’s cybersecurity framework if NIST issued healthcare-specific guidance about putting it to use. To date, HIMSS is the only healthcare-centric organization to submit comments in response to NIST’s recent request for information about awareness and use of the framework.

Financial

Financial Services

Activism

- A housing activist group held a ‘Renters’ Rights’ rally on October 21 in Baltimore, MD, demanding “a housing system that values human rights, a court system that values tenants’ rights to safe, adequate housing, and a Housing Authority that is committed to protecting public housing for the future.”

- A U.K. activist group launched a new fossil fuel divestment campaign targeting five of the country’s biggest banks. The campaign calls for consumers to issue an ultimatum to the banks to disclose and divest from fossil fuels, or else consumers will move their money out of their accounts.

- Occupy Wall Street endorsed a ‘Procession for the Innocents’ event to occur November 1st in NYC in which participants will conduct a procession from Union Square to St. Marks Church at 131 E 10th Street in remembrance of those who died from injustices such as police brutality.

- Hundreds of activists protested at bank branches across Australia on Saturday, October 18 while closing their accounts in protest over their banks’ financing of fossil fuels. Several hundred people in Melbourne and Sydney, plus hundreds more across fifteen locations around Australia and online took part in the national day of divestment action, organized by environmental advocacy groups. At least one bank in Melbourne declared a building lockdown as protesters became aggressive and the bank’s management feared for its employees’ safety.

-Activists on Wednesday, October 22 held protests at the Moscow Stock Exchange Forum in London, UK, condemning Western governments who are still maintaining business relationships with Russia and Putin’s government for bringing “thousands of deaths to the Ukrainian soil.”

- Housing activists held an anti-eviction protest last week outside a leading U.S. bank branch in Newark, NJ in support of an elderly, disabled woman who was evicted from her bank-owned property. The protesters claimed the eviction was "fraudulent and illegal."

- Housing activists held an anti-eviction demonstration at the 36th District Court in Detroit, MI on October 21 in support of a local homeowner facing eviction from her GSE-owned residential property.

- A Chicago, IL-based housing activist group plans to submit testimony to a United Nations fact-finding delegation responsible for investigating human rights violations in Detroit, MI. The group also plans to bring attention to the UN representatives the housing crisis in the Midwest and appeal for an investigation of the impact of the housing crisis, particularly neighborhoods hard-hit by the mortgage foreclosure crisis.

- An international environmental activist group created an online petition that calls for Wall Street executives to stop bankrolling the destruction of the Great Barrier Reef.

- An American activist group has purchased and abolished $3.8m of student debt owed by 2,700 students, paying just over $100,000. The activist group, funded by donations,
argues that student debt, which has spiraled to an estimated $1.2 trillion, is not usually as available to buy as other debts, such as unpaid medical bills.

- Protesting Israel's attack on Gaza past summer, a protestant church in Connecticut voted to divest from investment firms that invest in companies that operate on land that is occupied by Israel. The denomination to which the church belongs has around one million members across the US.

- Activists opposing the North American Free Trade Agreement (NAFTA) picketed outside the NAFTA meeting held in Seattle, WA on October 23.

**Information Security Risk**

- ATM skimmers are moving away from high-tech skimming devices and increasingly targeting aging ATM infrastructures in the United States and abroad using sophisticated software-based tools. The new attack trend targets ATMs from every manufacturer and multiple model lines. ATM attacks are most commonly occurring at standalone, unattended types of units where there is much easier access to the top of the machine as opposed to wall-mounted or attended machines.

- Dyreza/Dyre malware is exploiting old flaws in Adobe products to steal banking credentials and bitcoins. Both Reader and Acrobat are said to be affected by the malware, allowing hackers to enact man in the middle (MiTM) attacks and monitor online banking sessions, among other things. Hackers use spam messages masquerading as an invoice to infiltrate victims' systems, with a malicious PDF file hiding an executable that downloads a variant of the Dyreza malware. Most notably, one of the variants known as TSPY_DYRE.EKW can steal sensitive information by injecting malicious codes onto certain banking and bitcoin login webpages. The variant can also connect to specific STUN (Session Traversal Utilities for NAT) servers to determine the public IP address of the compromised computer. Countries most affected by this malware are Ireland, United States, Canada, Great Britain, and Netherlands.

- A new spam attack disguised as invoice message notifications is spreading the UPATRE malware that ultimately downloads its final payload- a banker malware related to the Dyreza/Dyre banking malware. Upon accessing any of the malicious URLs in the spammed messages, an Upatre variant detected as TROJ_UPATRE.YYJS is automatically downloaded in the system. Upatre is known for downloading other malware such as ZBOT and ransomware and typically uses spam as its infection vector.

- The Securities Industry and Financial Markets Association (SIFMA) called for the creation of a new inter-agency working group of regulators and the White House that would be tasked with developing consistent cybersecurity rules for the financial industry. The inter-agency harmonization working group could be led by the Office of Management and Budget, SIFMA said, would be charged with avoiding "unnecessary overlap" and making sure that any domestic requirements are consistent with international legal obligations.

- A leading U.S. office supply chain said last Monday, October 20, that it was investigating a "potential issue" involving its customers' credit card data in what could be the latest US retailer to fall victim to a payment card system security breach. Multiple banks said they had identified patterns of payment card fraud that suggested data had been stolen from several locations in the Northeastern US. The pattern suggested that the store cash registers in a handful of locations were infected with data-stealing malware similar to that used in other security breaches that allows thieves to create counterfeit cards.

- The FBI warned companies last Monday, October 20, that hackers stole more than 500 million financial records over the past 12 months, essentially breaking into banks without ever entering a building. The Bureau said about 35% of the thefts were from website breaches, 22% were from cyberespionage, 14% occurred at the point of sale when someone bought something at a retail store, and 9% came when someone
swiped a credit or debit card. About 110 million Americans, equivalent to about 50% of U.S. adults, have had their personal data exposed in some form in the past year.

- Microsoft warned users to uninstall the update, KB 2949927, released on Friday, October 17, even though there has been no mention of problems after the patch was installed. The software giant stated that this update has been removed from the Download Center because of an issue that has not been specified. The company said it is researching this issue and will post more information when it becomes available. It also recommended that customers who were experiencing issues with this update uninstall this update.

- A leading U.S. bank experienced a technical error that resulted in a subset of its customers getting charged twice when they attempted to use the new mobile payment service launched by a leading U.S. handset maker. The bank said that about 1,000 transactions were affected.

- Hackers are exploiting a zero-day vulnerability in Windows using malicious PowerPoint documents. Microsoft warns that the unpatched flaw is present in all supported versions of Windows except Windows Server 2003 and has already been abused in “limited, targeted attacks”. The bug (CVE-2014-6352) can be triggered by sending a specially crafted Microsoft Office file to intended targets before tricking them into opening the booby-trapped files.

- Security researchers saw an 183% increase in DDoS, DNS amplification attacks from January through August, which abuse recursive DNS resolvers. Recursive DNS resolvers look up a domain name and return an IP address, which can be called into a browser. But these types of servers return large amounts of data. Attackers abuse them by making requests but substituting the IP address of their victims. That directs a large amount of data to the victims, consuming up to 50 times more bandwidth, and thereby making it an “amplification” attack. The researchers warned that there are 28 million open DNS resolvers and they should be locked down and secured.

- Pro-Islamic hackers penetrated a stock exchange in Warsaw, Poland last week and gained “unauthorized” access to some archival log in data. Sources said the attack started on the server utp.gpw.pl from where the attack escalated and lasted for several days. The hackers declared in a series of posts published on a popular data dump site that all the governments that joined the bombing of the Islamic State are now their targets, specifically suggesting that Europe’s “peaceful life is over.” Further, the posts warned that “Your money, your information and your lives are under our control.”

- A cyberespionage group is using advanced spear-phishing techniques to steal email log-in credentials from the employees of military agencies, embassies, defense contractors and international media outlets that use Office 365’s Outlook Web App. The attack is effective because if victims know they had a legitimate OWA session opened before being timed out, they might not check if the URL changed before re-entering their credentials. In addition to using domain names that were very similar to those used by the targeted organizations for their real OWA log-in pages, in some cases the attackers even purchased legitimate SSL certificates so that victims’ browsers display the HTTPS secure connection indicators for the phishing sites. The phishing baits used by the attackers included well-known events and conferences that their victims were believed to be interested in.

- A leading American children’s toy manufacturer and retailer began notifying customers who made purchases on their website that their personal information may have been compromised in a breach that went undetected for 18 months. The company learned on September 9, 2014 that unauthorized individuals installed malicious software on the computer servers and took certain personal data entered by their customers. A forensic investigation revealed that the initial compromise occurred on March 31, 2013 and ended on October 6, 2014. The toy company warned that the malicious software could have compromised the personal information and other information of visitors that made purchases on their website, including name, address, website username and password, payment card account number, card expiration date, and payment card security code.
Researchers detected a 57% increase between August and September, 2014 in devices infected with Backoff malware, which scrapes a computer's RAM for leftover credit card data after a payment card has been swiped.

**Legal, Litigation, Regulatory Risk**

- An article published last week highlighted the lawsuit filed by the Virgin Islands Public Finance Authority (PFA) and the Government of the U.S. Virgin Island (GVI) against several leading U.S. financial firms for "incorrectly advis[ing] the PFA and GVI that the bond issue would have been tax-exempt." The suit seeks to recover $13.6 million payments to the IRS and all related costs.

- An article reported that a County Recorder of Deeds in Pennsylvania has filed a lawsuit against several of the nation's largest banks. The author wrote that the complaint asserts that the defendants conspired to circumvent the Recorder of Deeds Office and evade paying recording fees by creating a private electronic registry system known as Mortgage Electronic Registration Systems (MERS) to track mortgage assignments among themselves. The lawsuit alleges that property owners are no longer able to verify the true identity of the holders of their mortgages because of the banks' use of the electronic registry system.

- Occupy Wall Street commented that government auditors are investigating exclusive contracts held by two of the largest U.S. banks to provide financial services inside federal prisons. Reportedly, the banks issue debit cards to inmates when they are released that contain the balance remaining in their prison accounts. The post clarifies that it is unclear how much money the banks have made on the cards because the banks’ compensation comes from fees charged directly to former inmates.

- Industry insiders said top officials at the Treasury Department are discussing the need to bolster fortifications around a critical area of cybersecurity: outside vendors, which include law firms, accounting and marketing firms and even janitorial companies. Under discussion is a requirement that the banks put in place more stringent procedures and safeguards to make sure the outside firms have, at the least, basic defenses.

**Operational Risk**

- Bank of England had to shut down its Real Time Gross Settlement (RTGS) system last Monday, October 20th that handles about 575 billion pounds ($929 billion) of daily payments. The nine-hour disruption affected the same-day electronic transfers used by homebuyers, delaying some payments until late into the evening. The BOE extended the system’s operating hours and all 142,759 transactions submitted were eventually processed. Observers said the outage, which followed routine weekend maintenance, was the worst since software issues in 2007 prevented settlements for about six hours. The RTGS mechanism was suspended at 6:00 a.m. and remained offline until mid-afternoon.

- An article published last week said a Bitcoin company’s IPO is on track to launch on an Australia-based stock exchange early December, paving the way for more Bitcoin stocks to go public over the next few years. Currently the Bitcoin company runs a cryptocurrency arbitrage fund, but plans to expand into Bitcoin mining if the IPO succeeds. An industry insider said apart from the Bitcoin company being based in Australia, a major incentive for listing on an Australian stock exchange rather than in the United States is that the regulatory process for Bitcoin is further along there.

**Reputational Risk**

- A likely member of the Anonymous hacktivist collective, tweeted last week that an American post-trade financial services company "owns everything."

- An article published last week reported that Big Bank CEOs claim they never intended to break the law or engage in foreclosure fraud. However, the article claimed evidence such as internal documents obtained from a bank-backed venture several years ago
seem to directly contradict this claim. The article further highlighted that the mortgage-related fraud might not have been possible without a mortgage processing company that was created by the mortgage banking industry to simplify the mortgage process by using electronic commerce, alleging that the entity made it possible to bypass local processing for recording changes in title and loan ownership.

- An article reported that a female employee at a leading bank in U.K. alleged that her manager pressured her to have sexual relationships with executives. The article noted that similar incidents regarding sexual harassment at several leading U.S. banks were also reported in the past.

---

**Global Intelligence**

**China**

- Multiple employees at a Chinese drone company have landed in hot water after flying an unmanned aircraft over a Beijing suburb, sparking an air force hunt for the unidentified aerial intruder, according to local media.

- The China Labour Bulletin posted an article which discussed how three managers at a shoe factory in Guangzhou attempted to negotiate a compensation deal with management lawyers after learning the plant was closing. The article highlights the role of female workers and managers in collective bargaining within the manufacturing industry. Shuangye Metal Products Limited Company is based in Japan and is one of the largest components producers for the automobile company, Honda.

- Epoch Times reported that over a hundred workers went on strike at Shuangye Metal Products Limited Company in Dongguan from October 20-22. Workers protested due to docked overtime pay and social welfare benefits in arrears. The incident resulted in a violent confrontation with police, causing 8 to be arrested and 4 to be injured.

**Germany**

- Violent riots ensued over the weekend in Cologne, Germany, as approximately 4,000 football hooligans demonstrated against Salafist followers, which they suspect to be supporters of terror organization Islamic State. Right extremist groups are said to have participated in the events as well. While the demonstration was previously announced, the level of participation and violence seems to have come as a surprise to authorities. 44 police officers are reported injured and several police cars were damaged or destroyed. The events are seen as a new level of escalation after violent clashes between Kurds and Salafists earlier this month in Hamburg.

**Korea**

- On October 21 Smart Company reported that the Samsung General Labor Union has criticized Banolim, a victim’s rights group representing the families of Samsung employees who allegedly developed cancer while working at Samsung’s factories. The union says Banolim should join talks that are set to take place between the families of some victims and Samsung, overseen by a three-member mediation panel led by the respected former South Korean Supreme Court justice Ji-hyung Kim.

- On October 22 Korea Joongang Daily reported that Samsung confirmed it will compensate all of its leukemia-stricken employees after setting certain rules, refuting a local labor activist's claim that the company will only give money to those who participate in negotiations through a media group.

**North America**

- On October 20 Morning News USA reported that IBM has announced the sale of its global commercial chip making business to its partner Globalfoundries for 1.5 billion
USD. As part of the agreement, the company would turnover its microelectronics technology, intellectual property, and technologists to the unit’s acquirer, which will also serve as IBM’s exclusive provider of server processor semiconductor materials, including 22, 14, and 10 nanometer chips within the next 10 years.

- On October 21 Pando Daily reported that an antitrust lawsuit was filed last week against Oracle and Google. This makes the third such antitrust lawsuit to grow out the Techtopus Silicon Valley wage-fixing scandal.

- On October 22 Help Net Security published an article reported that Sucuri Security researchers have unearthed a malvertising campaign aimed at changing the DNS settings of home routers in order to lead users to questionable and potentially malicious websites.

- On October 24 Times Union reported that Electronics for Imaging Inc., a printing technology specialist, is paying more than $43,000 in back wages and penalties after labor regulators found eight employees brought from India were grossly underpaid and overworked while assigned to a specific project in the US. While assigned to the project, some of the Indian workers logged as many as 122 hours in a week without being paid overtime. As result, they received as little as $1.21 per hour.

**Vietnam**

- On October 23 Lao Dong News reported that thousands of workers from Vina Duke Company went on strike to demand for increase in wages, increase in subsidies, and increase in bath tags. After several days of negotiations, workers and company leaders failed to come to an agreement. Vina Duke, a textile bag manufacturer.

---

**Legal and Regulations**

- The Obama administration is delaying requirements for insurance companies to disclose records about enrollment data, claims denied and the amount consumers pay for specific services, reports Robert Pear for The New York Times.

- The U.S. Patent and Trademark Office (USPTO) will host a November 19, 2014, roundtable in Alexandria, Virginia, on the international harmonization of substantive patent law to secure stakeholder input on matters such as “the definition and scope of prior art; the grace period; and standards for assessing novelty and obviousness/inventive step.” USPTO’s focus is on “the successful reutilization of the examination work of one intellectual property office by another, or work sharing.” Attendees may register at the door, and the program will be Webcast.

- A new class action lawsuit alleges that on LinkedIn “any potential employer can anonymously dig into the employment history of any LinkedIn member, and make hiring and firing decisions based upon the information they gather, without the knowledge of the member, and without any safeguards in place as to the accuracy of the information that the potential employer has obtained.” The case is Tracee Sweet et al v. LinkedIn which was filed on October 4, 2014 in the US District Court for the Northern District of California.

**New gTLD Update**

- The General Availability phase for 2 new gTLDs, .market, .mortgage, will begin October 29, 2014.

- The General Availability phase for .saarland, a new gTLD will begin October 30, 2014.

- The Consumer Financial Protection Bureau (CFPB) has finalized a proposed rule that will eliminate the need for certain financial institutions to mail annual privacy notices to their customers, so long as the institutions publish their privacy notices online and
Worldwide

- United Kingdom: The Information Commissioner’s (ICO) new code of practice for surveillance cameras and personal information updates the previous 2008 CCTV code. It takes account of developments such as digital recording technology, portable technology, “drone” cameras and automatic number plate recognition systems, as well as “body worn” cameras used by organisations like the police. The code sets out the ICO’s guidance on how organisations should comply with data protection law when considering or using such technologies.

- Ireland: Bray District Court, yesterday, fined a firm of private investigators, and its two directors, €10,500 for unlawfully obtaining personal data. The court found that the directors had used ‘subterfuge’ to unlawfully obtain the addresses of credit union clients in arrears. The directors posed as a VEC and hospital worker to obtain the information, via telephone calls, from employees at the Department of Social Protection (seven cases), and the Health Services Authority (HSE) (sixteen cases). The Data Protection Commissioner stated that it will be engaging further with the Department of Social Protection and the HSE on the implications of the data security breaches which occurred, and the steps which should be taken to ensure such breaches do not recur.

- Spain: Pending final approval by the Congress, on October 15 the Senate gave green light to the reform of the Spanish Intellectual Property law. The reform has been considered as a short-term solution designed to address the severest gaps in policy prior to the final one which is supposed to come approximately within a year, following the recent adoption of Directive 2014/26/EU on collective management of copyright and related rights.

- European Union: The European Union’s independent data protection advisory body, the Article 29 Working Party has recently published an opinion (Opinion 8/2014) (the “Opinion”) on the ‘Internet of Things’. The Opinion addresses data protection and privacy concerns that arise from the use of networked or ‘smart’ products and clarifies the basis on which data protection law will apply to suppliers of such products. The Opinion specifically focuses on wearable computing (e.g. smart watches, glasses and clothing), quantified self (devices which measure personal information such as activity counters or sleep trackers), and home automation devices (e.g. smart light bulbs or washing machines).

Pharmaceuticals

- The U.S. Department of Homeland Security is investigating about two dozen cases of suspected cybersecurity flaws in medical devices and hospital equipment that officials fear could be exploited by hackers.

- One of the biggest attack campaigns against critical infrastructure since Stuxnet might not actually have been aimed at critical infrastructure. New research on the Dragonfly, a.k.a. Energetic Bear, attacks that were first reported by F-Secure in June poses the theory that the group’s true target was the pharmaceutical and biotechnology industry, not the energy sector. In a report released today by the signal transmission solution company Belden, Joel Langill, an industrial control systems security expert at RedHat Cyber, explains why he thinks Dragonfly was attacking small companies that supply original equipment manufacturers, which in turn supply the pharma-biotech sector.

- In the latest battle over the cost of prescription drugs, nearly 30,000 people have signed an online petition urging Roche to lower the price of its Kadcyla breast cancer treatment, which costs about $145,000 per patient in the U.K. and is considered too pricey for the National Health Service. The petition emerges two months after the U.K.’s National Institute for Health and Care Excellence rebuked Roche over the cost.
• A New York Times article reported that almost a decade ago, scientists from Canada and the United States reported that they had created a vaccine that was 100 percent effective in protecting monkeys against the Ebola virus. The researchers said tests in people might start within two years, and a product could potentially be ready for licensing by 2010 or 2011. However, the vaccine sat on a shelf for the past decade, due in part to what the article describes as a pharmaceutical “failure to produce medicines and vaccines for diseases that afflict poor countries.”

• The average board of directors in the biotech world is roughly 90% male, according to a new analysis, and more than half of all industry boardrooms host no women whatsoever, striking numbers that illustrate a sector that struggles with diversity.

• Almost a decade ago, scientists from Canada and the United States reported that they had created a vaccine that was 100% effective in protecting monkeys from Ebola.

• Brazil has unveiled the country’s first drug-tracking platform, a key piece of infrastructure that will connect regulators and drug registration holders as they implement the country’s 2013 National Drug Control System.

• European drugmakers say they support recent EU efforts to fight counterfeiting, but would like to see some changes to a provision that aims to catch fake products as they move across member-state borders.

Retail

• Staples is looking into a potential credit card data breach and has been in touch with law enforcement officials about the issue. The office supplies retailer said that if it turns up any data discrepancies during its investigation, customers won't be responsible for fraudulent activity on their credit cards as long as it is reported in a timely manner.

• Reuters reported that Sears Holding Corp is shuttering more than 100 stores and laying off at least 5,457 employees, investor website Seeking Alpha reported on Thursday. Sears spokesman Chris Brathwaite said the company would provide an update when it reports quarterly earnings next month. Reducing operations to the best performing stores is key to Sears' revival strategy, he said.

• BBC News reported that Tesco shares closed the day 6.5% down after the firm announced that its profits have been overstated by £263m. Tesco also announced that chairman Sir Richard Broadbent will be leaving.

• ZDNet reported that Staples is investigating a possible data breach which may have resulted in the loss of customer credit card data. At least half a dozen banking sources said there was "a pattern of credit and debit card fraud" which suggests that customer data may have been stolen from a number of Staples outlets.

• Family Dollar Stores on Tuesday announced that it has certified substantial compliance with both the Federal Trade Commission's second request regarding the acquisition by Dollar Tree, as well as the second request regarding Dollar General's bid for the company.

• Broadway World reported that Hallmark has partnered with Toys for Tots and pledged to donate $1.5 million in toys and funds to the organization this holiday season. Now through Christmas Eve, Hallmark Gold Crown stores are offering two ways customers can help the company provide donations and toys to families in need, which is listed on the company’s website.

• The list of retailers supporting Apple Pay during its launch in September was long and impressive, but in the weeks following the launch, some major retailers have blocked the service in favor of a competing option set to debut in 2015. According to user reports cropping up on Twitter, earlier this week, Apple Pay was operational at NFC
terminals at Rite Aid and CVS, both non-Apple Pay partners, but was reportedly disabled over the course of the last 48 hours.

Technology

- German airline Lufthansa is close to a deal to sell its IT infrastructure unit to IBM, including an outsourcing agreement for the services, as part of a shake-up of its technology activities, it said on Wednesday.

- A Chinese web monitoring group published a report saying Apple users in China have been targeted in a sophisticated and widespread attack by hackers seeking private user data stored on the iCloud service.

- A security researcher from Leviathan Security Group has identified a Tor exit node that was “actively patching binaries users download, adding malware to the files dynamically.”

- Cyber-criminals are exploiting a zero-day vulnerability using malicious PowerPoint documents sent as email attachments. The vulnerability affects several versions of Windows, from the aging Windows Vista to the very newest Windows 8.1, and lies within the operating system’s code that handles OLE (object linking and embedding) objects.

- Wearable computing devices such as smart watches and wrist bands are being pushed beyond their original purpose, and that is opening the door to new kinds of security risks, a former National Security Agency official said Tuesday.

- The FCC fined two phone carriers a total of $10 million, claiming the companies failed to protect the personal information of its customers.

- Russia’s communications regulator wants the right to carry out spot checks at Internet companies to make sure they are complying with a controversial law that forces them to collect data about popular bloggers.

- Google is rolling out refinements to its search algorithm designed to demote links to sites featuring content that allegedly infringes on copyrights.

Telecommunications

- United Airlines recently announced it plans to roll out Wi-Fi to its fleet of 200-plus two-cabin regional jets by next year. United will use Gogo’s ATG-4 Wi-Fi service and provide download speeds of up to 9.8 Mbps which is capable to support between 50 and 100 passengers.

- Fraud scams targeting the customers of several large American technology companies are seeking to provide password recovery and technical support to consumers for a weekly fee. These services, which target customers of Yahoo!, Google, Cisco, Apple to name a few, are otherwise offered for no charge by the company.

Entertainment
A new partnership by Nielsen and Adobe intends to fix some TV rating system limitations. A new system will allow the audiences to be measured across every device with an IP address which will dramatically expand the number of platforms that Nielsen's ratings can incorporate. The system will cover online content in addition to traditional video content.

Defense

C4ISRNet reports that the technology which allows online advertisers deliver content based on a user's location, browsing history, and interest are being used to send targeted malware attacks with attempts to infiltrate the United States defense contractors. Cyber security firm Invincea called the campaign "Operation DeathClick" and employs embedding malicious code in standard web ad.

Trend Micro researchers identified a cyberespionage operation dubbed “Operation Pawn Storm” that uses targeted emails and compromised Web sites to infect users in government, military, and media organizations with the SEDNIT (also known as Sofacy) malware.

As head of Naval Sea Systems Command (NAVSEA), Hilarides has come to the unpleasant realization that seemingly mundane data-collection for maintenance purposes has created vulnerabilities that could, in theory, be used to shut down key components on a sub.

The Chinese People's Liberation Army (PLA) is to introduce reforms aimed at improving the efficiency of military spending, the PLA Daily newspaper reported on 22 October. It said the measures will be introduced through a collaborative effort between several PLA agencies - including its procurement arm, the General Armament Department, and the General Logistics Department - in a bid to enhance the PLA's "battle effectiveness".

Northrop Grumman announced a 2% year-on-year decline in sales for the third quarter (Q3) to USD5.9 billion.

Lockheed Martin reported a reduction in sales for the third quarter of the year, and warned that the decline is expected to continue into 2015.

Boeing reported a 7% increase in year-on-year revenue to USD23.7 billion for the third quarter (Q3) of 2014 on 22 October, with revenue for the first nine months of 2014 increasing 5% to USD66.3 billion. Defence, Space, and Security revenue declined 2% in Q3 2014 to USD7.9 billion.

Russia is planning to increase defence expenditure by 32.8% to RUB3.286 trillion (USD80.4 billion) in 2015, according to the head of the State Duma Committee on Defence. If implemented the figure would represent the largest annual increase in defence expenditure since 2001.

A malicious campaign called “Operation DeathClick” focuses on specific targets such as defense contractors. The malvertising campaign has the ability to “target advertising to users based on location and interests.”

Researchers at Trend Micro released a paper on a cyber-espionage which targets the military, government, and media organizations around the world. The cyber-espionage campaign called “Operation Pawn Storm” have employed a variety of attacks such as “spear-phishing emails with malicious Microsoft Office documents lead to SEDNIT/Sofacy malware, very selective exploits injected into legitimate websites that will also lead to SEDNIT/Sofacy malware, and phishing emails that redirect victims to fake Outlook Web Access login pages,” writes senior researcher at Trend Micro.
A Congressional report reveals that China’s cyber espionage campaign against the United States continues despite the U.S. government’s efforts to end the problem. The report writes that “China to date has compromised a range of U.S. networks, including those of the DoD, defense contractors, and private enterprises,” and that the compromised weapons include the “Patriot Advanced Capability-3 air defense system, the F-35 and the F/A-18 fighter aircraft, the P-8A reconnaissance aircraft, the Global Hawk UAV, the Black Hawk helicopter, the Aegis Ballistic Missile Defense System, and the Littoral Combat Ship.”

A series of DDoS attacks allegedly from China appears to have been a run by a “well organized APT”. The experts from the Italian Tiger Security firm has called it “Operation Distributed Dragons” and that the threat actors have the capability to “evolve its techniques, tactics, and procedures (TTPs).” The bad actors initially targeted Linux servers, but the attacks also involved Windows machines and embedded devices with ARM architecture (e.g. Routers and IP cams), in this way the hackers are able to run DDoS attacks that reach traffic peaks of more than 200 Gb/s, without the use of amplification techniques.

Law Enforcement

- The Justice Department accused some Ferguson officials of leaking information to the media in an effort to support Officer Darren Wilson. In recent days, details of the investigation have appeared in local and national news coverage at a time when a grand jury decision is imminent on whether Wilson will be charged in the killing of an unarmed black teenager.

- Federal officials warned companies that hackers have stolen more than 500 million financial records over the past 12 months, essentially breaking into banks without ever entering a building. "We’re in a day when a person can commit about 15,000 bank robberies sitting in their basement," said Robert Anderson, executive assistant director of the FBI's Criminal Cyber Response and Services Branch.