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**

- Protestors have called for action at a conference being hosted by the oil and gas industry to recruit investors for new infrastructure in the Philadelphia area. Activists claim that such investments will aid companies that are polluting the city. A protest is planned on December 5, 2014 at 9:00 AM.

**Agribusiness**

- Syngenta AG, the world's largest maker of crop chemicals, said it will cut or relocate 1,800 jobs as Chief Executive Officer Mike Mack tries to tackle its cost base in countries such as Switzerland. The cuts are part of a program announced in February under which Syngenta will save $1 billion annually by 2018. About 500 of the positions
affected are in Basel, Switzerland, where the company is based.

**Insurance/Healthcare**

- Cybersecurity is one of the top 10 health technology hazards for 2015, according to a recent ECRI Institute report. Cybersecurity should be a top priority for healthcare organizations, especially with more facilities implementing EHRs and connecting to HIEs.

**Financial Services**

- Researchers discovered one of the most sophisticated pieces of malicious software ever seen. The bug, named Regin, is said to have been created by a nation-state and has been used for six years against a range of targets around the world. Once installed on a computer, it can do things like capture screenshots, steal passwords or recover deleted files. It has been used to spy on government organizations, businesses and private individuals, they said. The researchers also said the sophistication of the software indicates that it likely took months, if not years, to develop, and its creators have gone to great lengths to cover its tracks. Computers in Russia, Saudi Arabia and Ireland have been hit most.

**Global Intelligence**

- A U.S. multinational company will have to pay the Chinese government $140 million in back taxes and interest after authorities found what they called a major tax avoidance case, China’s state news agency said. The official Xinhua News Agency said Sunday the U.S. firm, which it referred to only as “Company M,” admitted to evading taxes when confronted by Chinese tax authorities and had agreed to pay 840 million yuan in back taxes and interest for an unspecified period. The firm also agreed to pay more than 100 million yuan in additional taxes every year, the report said. The description matches, at least in part, that of U.S. software giant Microsoft, a Fortune 500 company that set up its Chinese subsidiary Microsoft (China) Co. in Beijing in 1995.

**Legal and Regulations**

- Law enforcement agencies worldwide coordinated a global crackdown on cybercrime last week, arresting 118 people, Europol announced on Friday. The Europol, Interpol and Ameripol-coordinated action focused on airline ticket fraud and involved 45 countries, including the U.S., and more than 80 airports. The targets were airline tickets purchased using stolen or fake credit card data, a problem that costs the air travel industry $1 billion a year, Europol says. With representatives from airlines, credit card companies and industry associations, the operation identified suspicious transactions and sent alerts to transport hubs where officers could arrest suspects.

**Pharmaceuticals**

- A group of financially savvy computer hackers has been stealing data from more than 100 organizations, mainly targeting publicly traded health care, pharmaceutical and biotechnology companies, to gain insider knowledge and game the stock market. The news underscores the vulnerabilities of corporate computer networks and the many ways that cybercriminals use low-tech “social engineering” to further their aims. The cybercriminal group known as FIN4 “compromises the email accounts of individuals who regularly communicate about market-moving, nonpublic matters,” according to the “Hacking the Street” report from U.S. security firm FireEye, released Monday. The hackers are believed to be native English speakers based in North America or Western Europe.

**Retail**

- Two gunmen robbed a Cartier store in Paris before taking a hostage, leading police on a chase across the city and then taking cover inside a hair salon. There have been a number of high-profile robberies of luxury jewelry stores in France in recent years. A number have been attributed to the Pink Panthers, an international jewel thief network.
of mainly ethnic Serbs.

**Technology**

- The U.K. government is once again amping up counter-terrorism rhetoric against Internet companies, with Prime Minister David Cameron telling Parliament yesterday that digital communications firms' networks are “being used to plot murder and mayhem”, and asserting that web companies have a “social responsibility to act on this”.

**Telecommunications**

- The Federal Communications Commission (FCC) has announced that T-Mobile US has agreed to be more transparent over speeds its customers experience, particularly when it imposes speed restrictions and reductions.

**Entertainment**

- Sony Pictures is investigating whether a computer hacking attack on its servers may have been launched by North Korea in a bid to damage the studio's upcoming comedy “The Interview,” sources told the tech site re/code.

**Defense**

- The Department of Homeland Security is poised to ditch all records from a controversial network monitoring system called Einstein that are at least three years old, but not for security reasons. DHS reasons the files -- which include data about traffic to government websites, agency network intrusions and general vulnerabilities -- have no research significance.

**Law Enforcement**

- Spurred by the Ferguson, Missouri shooting, President Barack Obama is calling for $75 million in federal spending to get 50,000 more police to wear body cameras that record their interactions with civilians. However, Obama is not seeking to pull back federal programs that provide military-style equipment to local law enforcement.

---

**Energy**

- A 2-day meeting of anti-fracking activists will be held to develop a nationwide anti-fracking picture in Leicester, UK on December 13, 2014.

- Protestors have called for action at a conference being hosted by the oil and gas industry to recruit investors for new infrastructure in the Philadelphia area. Activists claim that such investments will aid companies that are polluting the city. A protest is planned on December 5, 2014 at 9:00 AM.

- Over the past four years, the Unist'ot'en clan of the Wet'suwet'en nation have literally built a strategy to keep three proposed oil and gas pipelines from crossing their land. Concerned about the environmental damage a leak could cause on land they've never given up, they've constructed a protection camp to block pipeline companies. As opposition to the development of Alberta's tar sands and to fracking projects grows across Canada, with First Nations communities on the front lines, the Unist'ot'en camp is an example of resistance that everyone is watching.

- The Obama administration on November 21, 2014 released its latest Unified Agenda, updating its coming regulatory priorities, including moving ahead on several regulations impacting coal mining companies. The industry faces at least 10 new regulations identified in the semiannual agenda and will be further impacted by regulations that target coal-burning utilities, including those aimed at limiting
• Fiscal incentives for carbon capture should be part of the global climate change agreement that replaces the Kyoto Protocol, 56 countries belonging to the U.N. Economic Commission for Europe (UNECE) said in a statement on Tuesday. The recommendation by the UNECE member states puts the issue formally on the table for a meeting of the U.N. Framework Convention on Climate Change in Paris in December 2015, which aims to agree a legally binding treaty to replace Kyoto.

• The sharp increase in oil trains in Washington has prompted the state to rethink its emergency response plans, Copeland said. That process continues, and some officials have acknowledged that the state is ill-prepared for a major oil-by-rail disaster. A series of derailments and explosions have heightened worries since last year. Several were linked to Bakken crude oil from North Dakota, which accounts for much of the crude now moving through Washington. Multiple reports and analyses have suggested Bakken oil is more dangerous than other types of crude. “It’s not just this new mode. It’s a new type of oil,” Copeland said. “It’s a more volatile oil than we’re used to dealing with. It takes new resources. It takes new training.”

---

**Agribusiness**

• Final unofficial results in Oregon show the GMO labeling initiative failed by 809 votes out of 1.5 million ballots. The split in votes "is within the margin that would trigger an automatic recount," said the Secretary of State's office.

• The new H5N8 avian influenza confirmed in Germany, the Netherlands and Britain "poses a significant threat to the poultry sector, especially in low-resourced counties situated along the Black Sea and East Atlantic migratory routes for wild birds", said two international groups, the UN Food and Agriculture Organization and the World Organization for Animal Health, known by its French abbreviation OIE. The H5N8 strain was reported earlier this year in China, Japan and South Korea. FAO and OIE said wild birds may have played a role in the rapid spread of the highly pathogenic virus.

• The first case of porcine epidemic diarrhea virus was confirmed in Hawaii, on a farm in Waianae Valley on Oahu, says The Pig Site, and the state Agriculture Department has issued a quarantine order against movement of hogs on the west side of the island.

• Syngenta AG, the world's largest maker of crop chemicals, said it will cut or relocate 1,800 jobs as Chief Executive Officer Mike Mack tries to tackle its cost base in countries such as Switzerland. The cuts are part of a program announced in February under which Syngenta will save $1 billion annually by 2018. About 500 of the positions affected are in Basel, Switzerland, where the company is based.

---

**Insurance/Healthcare**

• As hospitals and healthcare systems continue to implement new technologies, it is likely just a matter of time before interoperability is a hurdle they must overcome as well. Data sharing and the safe transport and exchange of patients’ protected health information (PHI) is a critical step that healthcare organizations need to be able to securely take. Florida’s Memorial Healthcare System knew that it needed to implement a secure interoperability option when it decided to connect with Henderson Behavioral Health. Henderson can now receive confidential emergency room referrals from Memorial. The move was done to more effectively treat patients, save money, and ensure care continuity.
• Making good on a promise to beef up scrutiny of the HITECH Act financial incentive program for electronic health records, a federal watchdog agency says a recent audit found that the Massachusetts Medicaid program overpaid 13 hospitals a total of nearly $2.7 million.

• The American Medical Informatics Association is asking Congress to amend a central federal healthcare privacy rule, in order to give medical researchers access to patient records without their consent. A see-saw battle has been waged at the federal policy level for more than a decade over patient consent regarding medical records, with patient privacy advocates arguing that control over information about one’s self is the definition of privacy.

• Despite their substantial concerns about privacy and security, a large majority of U.S. consumers support the use and exchange of electronic health records by their healthcare providers. About 75 percent of consumers support the use of EHRs, according to recently released findings of a survey of more than 1,700 American consumers conducted for the Office the National Coordinator for Health IT.

• Cybersecurity is one of the top 10 health technology hazards for 2015, according to a recent ECRI Institute report. Cybersecurity should be a top priority for healthcare organizations, especially with more facilities implementing EHRs and connecting to HIEs.

• Healthcare data breaches are unfortunately becoming a common scenario for hospitals, health systems and individual care providers. The ramifications of a security breach can be far-reaching, and organizations might have to work to prove themselves once again capable of keeping patients’ protected health information (PHI) secure. But just how long can healthcare data breaches affect organizations?

• A new industry alliance is promoting software specifications that could help pave the way for secure national exchange of health data, including making sure the right patient is matched with all the right records.

• The Centers for Medicare & Medicaid Services (CMS) recently announced that eligible hospitals (EHs) and critical access hospitals (CAHs) would have until December 31 rather than November 30 to complete their meaningful use attestation for the Medicare EHR Incentive Program 2014 reporting year.

• As healthcare technology continues to evolve, the need for facilities to have comprehensive and current cybersecurity measures continues to increase. In fact, the majority of healthcare executives report that their spending on cyber threats has increased, according to recent IDC research.

• An ongoing legal dispute between the Texas Health and Human Services Commission and its former contractor, Xerox, has led the state agency to report to federal authorities that the business associate was responsible for a data breach affecting 2 million individuals. The dispute, which arose when the state ended its contract with Xerox, serves as an important reminder of the importance of preparing for the ending of relationships between covered entities and BAs by including specific details about data return or destruction in business associate agreements.

• A severe storm struck the Jacksonville, Florida, area early last week, causing significant damage to many properties. The majority of this damage was caused to roofs, which may present a major problem for those that fell victim to the storm. The Florida Association of Public Insurance Adjusters has issued a warning to those affected by the storm, cautioning them against fake insurance adjusters. In the wake of major storms, fraudulent adjusters often seek to take advantage of those that have had their properties damaged.
Financial Services

Activism

- Occupy Wall Street activists held a protest on November 25, 2014 against the CEO of a leading U.S. bank and the US Attorney General outside the bank’s headquarters in NYC. The protest was held in support of a former bank employee turned whistle blower who claimed the Attorney General could have prosecuted the bank criminally, but refused and instead negotiated a $13 Billion settlement.

- Housing activists promoted support for a local family facing eviction from their GSE-owned home in Swarz Creek, MI, claiming the GSE is refusing to work with the family to let them stay in their home.

- Activist groups will host a housing conference to occur in Seattle, WA on December 12-13, 2014. The purpose of the conference is to unite activist groups to fight displacement, get a fast-paced primer on strategies and tactics, identify priority campaigns for Seattle, share skills, and strengthen ties with groups.

- A housing activist group issued a call to action targeting a mortgage lender specializing in servicing high-risk loans for the lender’s alleged fraudulent and abusive business practices.

- Several tweets called to set fire to nationwide bank facilities after the Grand Jury’s verdict on Police Officer Darren Wilson, specifically referencing several major U.S. banks.

- Occupy Wall Street is planning upcoming actions “from here into 2015,” and will host planning meetings from November 28, 2014 through January 2, 2015 in NYC. Planning actions appear to be focused on 1) Human Rights-Housing, 2) Democracy and Justice, 3) The Environment, and 4) Labor.

- A ‘Millions March’ event will occur December 13, 2014 in NYC in which participants will demand that the Department of Justice pursue federal charges against Police Officer Darren Wilson in the murder of Michael Brown.

- Occupy Wall Street is planning a day of action for low wage workers on December 4, 2014 in NYC with several actions occurring throughout the city.


- Police cleared the remaining barricades from the shopping streets of Mong Kok, one of Hong Kong’s largest protest sites, on November 26th and arrested two pro-democracy leaders as authorities stepped up their efforts to end the two-month-long civil disobedience campaign.

Information Security Risk

- Beginning with the Federal Reserve Bank of St. Louis, hackers on November 22, 2014 launched attacks against St. Louis, MO area banking websites in solidarity with Ferguson, MO, under the flag of #OpFerguson.

- Hackers launched cyber-attacks on November 24, 2014 against several financial institutions, corporations, and government agencies across the nation following the Grand Jury’s verdict on police officer Darren Wilson.

- Researchers discovered one of the most sophisticated pieces of malicious software
ever seen. The bug, named Regin, is said to have been created by a nation-state and has been used for six years against a range of targets around the world. Once installed on a computer, it can do things like capture screenshots, steal passwords or recover deleted files. It has been used to spy on government organizations, businesses and private individuals, they said. The researchers also said the sophistication of the software indicates that it likely took months, if not years, to develop, and its creators have gone to great lengths to cover its tracks. Computers in Russia, Saudi Arabia and Ireland have been hit most.

- Researchers identified a new high-risk Android app called ANDROIDOS_STIP.A in Chile that can be used to hack into the user’s RFID bus transit card to recharge the credits. The researchers found that when the app runs on an NFC-enabled device, it can read and write to these types of cards.

- A new study said nearly half of all web application cyber-attack campaigns target retail applications. The study found that 40% of all SQL injection attacks and 64% of all malicious HTTP traffic campaigns target retail websites. This is largely due to the data that retail websites store – customer names, addresses, credit card details – which cyber criminals can use and sell in the cyber-crime underworld. Retail sites suffered twice as many SQL injection attacks in comparison to other industry sectors. Other findings from the study revealed that websites containing consumer information, which require some form of log-in credentials, suffer up to 59% of the attacks.

- Reports said fears are growing that Iran will unleash cyber warfare on U.S. companies if negotiators are unable to reach a nuclear deal that would require Tehran to limit its nuclear program. Cyber-attacks from Tehran dropped after the U.S., Iran and other countries agreed to an interim nuclear deal in 2013, but observers expect a new offensive if discussions fall apart. U.S. financial firms, oil and gas companies and water filtration systems could be among the companies targeted, some observers said. Researchers describe Iran as a close fourth behind the U.S., Russia and China in terms of its ability to launch cyber-attacks.

- A Canadian broadcasting company reported that it had “inadvertently” received 18 pages of “detailed tax information” pertaining to hundreds of primarily rich and famous Canadians. The records were from a Canada Revenue Agency spreadsheet spanning from 2008 to 2013, and they included home addresses and information about tax credits granted for charitable donations.

- A new study said more than 6 million email accounts and their credentials have been compromised by criminals over the last three months. The report claimed around 150,000 account credentials are leaking each month. On average, the current or previous passwords of about 4% of emails are available on the e-crime scene, and that right now it has spiked to 6%. So, a company with 1,000 employees would have 60 workers with leaked historic account details, said the report.

**Legal, Litigation, Regulatory Risk**

- An article reported that the United States Securities and Exchange Commission agreed to partially waive additional sanctions that could have been imposed on a leading U.S. bank, following a record settlement in August over the sale of residential mortgage-backed securities. The article said that the bank will be allowed to continue selling private shares for clients for 30 months, during which time they will be required to hire an independent consultant to monitor their compliance in this area. The bank will need to reapply with the SEC in order to receive a full waiver on this sanction.

- A leading UK investment bank was fined 56 million pounds ($88 million) by British regulators for the 2012 collapse of its computer system that left millions of customers without access to their accounts for weeks.

**Operational Risk**

- Researchers demonstrated that it is possible to figure out the IP address and therefore
the identity of individuals who use Bitcoins to pay for online transactions. The researchers explained that Bitcoins do not protect the IP addresses of users, and these can be linked to the user's transactions in real time, even if the client uses different pseudonyms for each transaction. They added that Tor is not really able to protect a Bitcoin user's identity from a would-be hacker either, as the Bitcoin's built-in denial of service (DoS) protection can be exploited. The researchers claimed that a hacker could discover the identity of a Bitcoin user by using several computers and spending just under $1,870 on such a deanonymisation attack.

- An Asian stock exchange has indefinitely shelved a plan to hold a two-hour evening session, which was being considered as a way for the bourse to better compete with rivals in Europe and the United States. An exchange spokeswoman said some opponents worried about how fairly shares would be priced given the expected weak trading volume in the evening. Additionally, some domestic brokers and institutional investors cited extra staff costs would outweigh the benefits of the exchange's proposed two-hour evening session.

Reputational Risk

- An article reported that a leading U.K. bank has come under fire for its holdings in an Israel-based international defense electronics company, as it is the owner of $2.9 million worth of shares in the defense firm. As a result, more than 1.7 million people have so far signed a petition calling on the bank to divest from projects that allegedly finance "illegal" settlements and the "oppressive occupation" of Palestinians. Anti-Israeli campaigners have occupied and protested at bank branches across the UK.

- An environmental whistle blower group published a report of the coal portfolio of the world's largest sovereign wealth fund, the Norwegian Government Pension Fund Global (GPF). The report reveals that the Pension Fund's holdings in the coal industry are much larger than previously acknowledged, and that GPF now ranks amongst the top 10 investors in the global coal industry.

Global Intelligence

China

- A Chinese news outlet reports 38% of the enterprises with online services have experienced DDoS attacks over the past 12 months.

- A Chinese news outlet reports the 3rd generation of the "Elder Trojan", which infected one million mobile devices are responsible for multiple malicious application surfaced over past months. The 3rd generation Elder Trojan are able to replace the phone system files deceptively, download large number of malicious programs and is extremely difficult to remove.

- A Chinese news outlet reports a malware spreading via text messages by send user a link claiming that it contains a picture of the user and lure user to open the link. Once the link is opened, malicious application will be downloaded to the mobile device. The malware is able to randomly select 20 contacts on the infected devices and send the same link to the 20 contacts.

- A Chinese technology outlet reports a new version of "NotCompatible.c" emerged and potentially targeting enterprises networks. According to the article, it is capable of data redundancy and encryption to protection itself.

- A Chinese technology news outlet reports seven largest digital crime trends is Asia. Due to the increasing number of internet users, Asia has become a hot spot for hacktivist activities.
Chinese news outlets reported that over a thousand workers at Daxin Furniture Limited Company in Dongguan went on strike due to poor cafeteria food quality. According to the article, the strike ended when the company promised workers an additional 300 Yuan added to their monthly paychecks.

A U.S. multinational company will have to pay the Chinese government $140 million in back taxes and interest after authorities found what they called a major tax avoidance case, China’s state news agency said. The official Xinhua News Agency said Sunday the U.S. firm, which it referred to only as “Company M,” admitted to evading taxes when confronted by Chinese tax authorities and had agreed to pay 840 million yuan in back taxes and interest for an unspecified period. The firm also agreed to pay more than 100 million yuan in additional taxes every year, the report said. The description matches, at least in part, that of U.S. software giant Microsoft, a Fortune 500 company that set up its Chinese subsidiary Microsoft (China) Co. in Beijing in 1995.

**Germany**

According to a study in Germany, the use of social media among teenagers between the ages of 12 and 19 decreased by ten per cent over the last year. Approximately 73 per cent of this age group are using social media, around 45 per cent for the youngest age group, 12 to 13 years. However, some platforms show increases, e.g. WhatsApp and Instagram.

**Malaysia**

MTUC posted on its blog criticizing the way the police and and the Home Ministry handling the labor dispute at JCY HDD Technology Sdn Bhd (JCY) by simply calling the abuse as "just a misunderstanding due to language barrier". JCY HDD in Johor is roughly 425 miles from Intel Penang.

The human right activist, Charles Hector criticized the Malaysian government statements on JCY HDD Technology Sdn Bhd (JCY) did nothing wrong that caused a riot on company property, and it was just a misunderstanding due to language barrier among the workers. MTUC has step up and challenge this statement as well. JCY HDD in Johor is roughly 425 miles from Intel Penang.

A Malaysian news outlet report the National Population and Family Development Board (LPPKN) urged employers in Malaysia to consider implementing flexible working hours to enable employees to spend more times with their family.

A Malaysian news outlet reports the population of foreign workers without permit in Malaysia has reached an estimate of 6.7 million.

A Malaysia news outlet reports the employees in private sector can look forward to salary increment in 2015 due to the implementation of Good and Services tax in April 2015.

A Malaysian news outlet reports nearly 100 railroad workers from KTMB (Malaysian National Train Service) who were terminated for protesting against the company's management will be reinstated.

**North America**

Business Insider reported that HP has laid off 41,000 people (with about 9,000 people left to go) under the current downsizing plan for 2014. HP hinted that more layoffs could be coming with its plans to separate itself into two companies.

Time of Israel reported that negotiations between state officials and representatives of the powerful Histadrut labor union broke down Tuesday, November 25, 2014, only one day after the parties held their first meeting, as the two sides were unable to reach an agreement on potentially raising the low minimum wage. However, a meeting between the Histadrut and the Finance Ministry is scheduled for Wednesday to discuss the widespread use of temporary workers for cleaning and security services. The Hisadrut
labor union threatened to launch a general strike over minimum wage last week. If Nissenkorn were to declare such a measure, there would be a two-week period before he could put the strike into action.

- Huffington Post reported that the tech worker shortage problem that tech CEOs complain about does not exist. The article reported that the real problem is not that there aren't enough qualified workers to do the tech jobs, but that tech companies don't want to pay people enough money to do them. A study conducted by Hal Salzman found that 50 percent of computer-science college students don't enter the tech industry after graduation. Thirty-two percent of the students Salzman surveyed said there weren't enough tech jobs available -- countering any idea of a worker shortage. Fifty-three percent of students said they “found better job opportunities outside of IT occupations.”

- The San Jose Mercury News reported that As organized labor expands its efforts in Silicon Valley, a local union and civil rights activist the Rev. Jesse Jackson are pushing for better working conditions for the security guards who work at Apple's campus. United Service Workers West, a regional arm of the Service Employees International Union, hopes to unionize security guards who work on Apple’s campus, and in the short term is asking Apple to use a different security contractor.

**Vietnam**

- Yahoo! Finance reported that the Vietnamese government issued a statement reporting that Thai Nguyen province has granted Samsung the license to invest $3 billion to expand its production in northern Vietnam.

- Lao Dong News reported that Vietnam’s Ministry of Labor, Invalids and Social Administration submitted 2 proposals regarding holiday leave for Lunar New Year 2015, the year of the sheep. One proposal proposed 7-days-holiday-leaves for workers and the other proposed a 9-days-holiday-leaves for workers. According to the article, the majority of National Assembly members, economist, sociologists, business owners, and union officials agreed that the 9-day-holiday leave would be better.

- Lao Dong News reported that many business has cut corners on workers' meals to decrease cost. In 2014 Ho Chi Minh had 70 strikes, 28 of those strikes were related to the quality of the meals. In October 2014 alone, 2 strikes occurred due to the quality of food served. On October 27, 2014 nearly 1,000 workers at T.O. Company went on strike requesting that the company reform the quality of the food it serves. Before that incident, 4,000 workers from Vina Duke Company also went on strike over the quality of the company's meals.

---

**Legal and Regulations**

- The Supreme Court is weighing the free-speech rights of people who use violent or threatening language on Facebook and other social media. The justices will hear arguments Monday in the case of a man who was sentenced to nearly four years in prison for posting graphically violent rap lyrics on Facebook about killing his estranged wife, shooting up a kindergarten class and attacking an FBI agent. Lawyers for Elonis argue that the government must prove he actually intended his comments to threaten others. The government says it doesn’t matter what Elonis intended; the true test of a threat is whether his words make a reasonable person feel threatened. The case is Elonis v. United States, 13-983.

**Healthcare**

- The Massachusetts Attorney General announced Friday that her office had reached a settlement with Beth Israel Deaconess Medical Center (BIDMC) surrounding a 2012 data breach in which a physician’s unencrypted personal laptop containing patient and
employee information was stolen from BIDMC’s grounds. Under the terms of the settlement, BIDMC agreed to pay a $100,000 fine and take additional measures to ensure compliance with state and federal data security requirements, including encrypting, physically securing and tracking all portable devices, and training employees on how to handle patients’ personal and protected health information (PHI). The data breach at BIDMC and the resulting settlement demonstrate the importance that covered entities must place on adequately securing portable devices that contain sensitive patient information, as well as carefully adhering to both state and federal data security and breach notification requirements. Additionally, this settlement demonstrates the importance of encryption in avoiding a data breach.

**Worldwide**

- Law enforcement agencies worldwide coordinated a global crackdown on cybercrime last week, arresting 118 people, Europol announced on Friday. The Europol, Interpol and Ameripol-coordinated action focused on airline ticket fraud and involved 45 countries, including the U.S., and more than 80 airports. The targets were airline tickets purchased using stolen or fake credit card data, a problem that costs the air travel industry $1 billion a year, Europol says. With representatives from airlines, credit card companies and industry associations, the operation identified suspicious transactions and sent alerts to transport hubs where officers could arrest suspects.

- Germany’s parliament confirmed that a legal loophole allows the nation’s foreign intelligence service to spy on German citizens who are working abroad for foreign companies.

- Polish government auditors found that state agencies and government institutions are not equipped to deal with cyberattacks and online threats.

**Pharmaceuticals**

- A group of financially savvy computer hackers has been stealing data from more than 100 organizations, mainly targeting publicly traded health care, pharmaceutical and biotechnology companies, to gain insider knowledge and game the stock market. The news underscores the vulnerabilities of corporate computer networks and the many ways that cybercriminals use low-tech “social engineering” to further their aims. The cybercriminal group known as FIN4 “compromises the email accounts of individuals who regularly communicate about market-moving, nonpublic matters,” according to the “Hacking the Street” report from U.S. security firm FireEye, released Monday. The hackers are believed to be native English speakers based in North America or Western Europe.

- China is considering lifting price caps on most drugs sold in the country, Bloomberg News reports, citing a proposal sent to drug industry groups. The National Development and Reform Commission would let prices be set by the market and impose measures to keep drug costs from spiking.

- A fifth person has pleaded guilty to participating in a 2010 heist at an Eli Lilly warehouse Connecticut that prosecutors say involved up to $100 million in prescription drugs.

- Actavis Plc, which this month agreed to buy Allergan Inc. for $66 billion, plans to cut employees and expand in China, executives from the companies said. Actavis Chief Executive Officer Brent Saunders said there are overlaps in corporate functions, including human relations and finance, though he hasn’t yet quantified how many positions will be eliminated.

- A Novartis scientist who engaged in research misconduct has been banned from receiving federal funding for three years and has also been dismissed by the drug
Retail

- Web shoppers bought more often, but spent less per order during the weekend before Thanksgiving compared with the same period in 2013, IBM reports.

- An Ohio state legislator, Mike Foley, wants companies to pay workers three-times their normal hourly wages on Thanksgiving.

- Samsung Electronics is planning for a large-scale workforce reduction of their IT and Mobile (IM) departments. Approximately 6000 Galaxy Series employees will be moved to other departments or redeployed.

- The London Evening Standard reported that telecommunications company BT revealed that it is in talks over a takeover of either mobile rival O2 or EE in a deal worth as much as £10 billion. The deal could see the foreign owners of the mobile networks taking a 20% stake in BT in return for their UK arms.

- In a press release, MasterCard outlined its vision for online payments beyond passwords, making life simpler for cardholders while increasing security. The company has been leading the co-creation of a new authentication standard, which when adopted, will be the largest wholesale upgrade to online payment security. It is designed to benefit consumers, banks and merchants alike, with invisible authentication and far fewer prompts for passwords.

- Teku Blog reported that Wal-Mart is being forced to sell PlayStation 4 consoles in the United States for $99 (£58), with the help of Amazon. The retail giant recently brought in a policy meaning they will price-match many online retailers including Amazon.

- Two gunmen robbed a Cartier store in Paris before taking a hostage, leading police on a chase across the city and then taking cover inside a hair salon. There have been a number of high-profile robberies of luxury jewelry stores in France in recent years. A number have been attributed to the Pink Panthers, an international jewel thief network of mainly ethnic Serbs.

- Just as the U.S. holiday shopping season kicks off, Verizon’s Enterprise Solutions unit has introduced the Verizon Retail Index, a new tool to give members of the retail, shipping and transportation industries another point of view about online consumer habits.

- Home Depot is facing at least 44 lawsuits related to a data breach at the home-improvement retailer that involved the theft of payment card information and customer e-mail addresses. The retailer warned it was facing dozens of civil lawsuits in the U.S. and Canada, according to a filing with the Securities and Exchange Commission, as well as investigations by a number of state and federal agencies.

Technology

- Smoking will not only damage your health but also your computer, as e-cigarettes manufactured in China are reportedly being used to spread malicious software through the USB connection used to charge the device.

- A new technique used to exfiltrate data has been discovered by uploading a video to the cloud services as a way to move data out of compromised networks without detection. The technique utilizes steganography where encrypted data is encoded into video files and uploaded to trusted or unmonitored video sharing services and then...
• A high-risk Android app, known as ANDROIDOS_STIP.A has been detected in Chile. The app was found to be distributed through forums and blogs and can be used to hack into the user’s RFID bus transit card to recharge the credits.

• A man-in-the-middle attack called “DoubleDirect” is currently being used in the wild to redirect mobile connections to major websites such as Google, Facebook, and Twitter. The method relies on ICMP to redirect packets to change the routing tables of a host; these are used by routers to announce a machine of a better route for a certain destination.

• Malicious Adobe Flash (.SWF) files are being incorporated into exploit kits like the Magnitude Exploit Kit, the Angler Exploit Kit, and the Sweet Orange Exploit Kit.

• Europe’s Article 29 Working Party, the body comprised of data protection representatives from individual Member States of the European Union, has now published guidelines on the implementation of the so-called ‘right to be forgotten’ ruling, which was handed down by Europe’s top court back in May.

• The European Parliament sent a message on Thursday: they support the idea of breaking up Google. While the search giant was not mentioned by name, members voted 384 to 174 (with 56 abstentions) in favor of a set of measures encouraged to drive more tech growth across the European Union. Among those measures: a resolution to enforce European competition rules against online companies that are deemed to be abusing dominant positions in search. Specifically, “MEPs also call on the Commission ‘to consider proposals with the aim of unbundling search engines from other commercial services’ in the long run.”

• The U.K. government is once again amping up counter-terrorism rhetoric against Internet companies, with Prime Minister David Cameron telling Parliament yesterday that digital communications firms’ networks are “being used to plot murder and mayhem”, and asserting that web companies have a “social responsibility to act on this”.

• Twitter is now collecting information about the apps installed on users’ devices in order to better target and tailor advertising and other content to them.

---

**Telecommunications**

• Britain’s biggest telecoms service providers have filed a complaint to media regulator Ofcom demanding greater competition in the business broadband market, where they say BT has an effective monopoly.

• The Federal Communications Commission (FCC) has announced that T-Mobile US has agreed to be more transparent over speeds its customers experience, particularly when it imposes speed restrictions and reductions.

• According to a recent lawsuit filed by music publishers; a push is being made that downloading music illegally is the fault of ISPs who aren’t punishing pirates. The complaint insinuates that it’s the responsibly of the ISP to end service of repeat offenders based on the Digital Millennium Copyright Act.

---

**Entertainment**
Sony Pictures is investigating whether a computer hacking attack on its servers may have been launched by North Korea in a bid to damage the studio’s upcoming comedy “The Interview,” sources told the tech site re/code.

Netflix recently announced the return of its highly successful, exclusive, program will be back for its third season. The premiere is set for February 27, 2015.

The St. Louis Police Officers Association is urging the NFL to take action against five St. Louis Rams players, who entered the field for player introductions with their hands raised in the air. This pose has become a fixture of the protests following the police killing of Michael Brown in August. The SLPOA released a statement expressing their disappointment in the action of the players for being tasteless, offensive and inflammatory.

### Defense

- China’s State Council has made an unprecedented and unexpected move to allow private sector companies in the country to bid for defense contracts.

- Highly anticipated federal rules on commercial drones are expected to require operators to have a license and limit flights to daylight hours, below 400 feet and within sight of the person at the controls, according to people familiar with the rule-making process.

- The Department of Homeland Security is poised to ditch all records from a controversial network monitoring system called Einstein that are at least three years old, but not for security reasons. DHS reasons the files -- which include data about traffic to government websites, agency network intrusions and general vulnerabilities -- have no research significance.

- With more than 10 million purported attempts to break into Pentagon systems and servers each day, it was not surprising when the White House confirmed that individuals thought to be working for the Russian government attempted to hack its servers. The White House is in good company with NATO, the Ukrainian government and U.S. defense contractors all detecting similar activities. Responding to the attack, anonymous officials indicated that the intruder didn’t damage any system or gain access to the “classified network.”

- CIA Director John Brennan is considering sweeping organizational changes that could include breaking up the separate spying and analysis divisions that have been in place for decades to create hybrid units focused on individual regions and threats to U.S. security, current and former U.S. intelligence officials said.

- The recently discovered Regin malware lets its creators to quickly add new capabilities or customize it to avoid specific defenses. Sources indicate that the malware contains attributes from other sophisticated malware families such as the Flamer and the Weevil (The Mask) and that the malware’s objective is surveillance. The malware appears to target telecom operators such as GSM networks, government institutions, multi-national political bodies, financial institutions, research institutions and “individuals involved in advanced mathematical/cryptographical research” from various regions of the world except for the U.S. and U.K.

- A cyber-espionage campaign called "APT 3", believed to be culprits behind the Op Clandestine Fox is now running a new campaign called "Operation Double Tap." The hackers exploited an IE zero-day vulnerability in a series of targeted attacks, now the ATP3 group is exploiting a series of flaws in Microsoft OS, including the CVE-2014-6332 vulnerability recently patched that was exploitable for 18 years before the update. APT 3 may have exploited the Windows OLE bug and also another Windows privilege escalation vulnerability (CVE-2014-4113). The joint use of the two
vulnerabilities suggests that APT3 has apparently moved from leveraging zero-day exploits, to attacking targets with “known exploits or social engineering”.

Law Enforcement

- Islamic State supporters are calling on lone-wolf attacks in areas where law enforcement is distracted by unrest in the wake of the Ferguson grand jury decision. The supporters are using social media to spread the message. In one tweet, Al Nusra Al Maqdisiyaa, a popular group of pro-ISIS activists, wrote “O lone mujahid, you must use the breakdown of security in #Ferguson to increase the burning in America. They are squabbling over worldly [matters], so you send them to hell! #ISIS.” Another tweet from ISIS supporters read, “O supporters of the Islamic State in America, what is happening in #Ferguson is a valuable opportunity that will not return. Rise up and engage them with themselves, away from the mujahideen. Spill their blood in the roads and in the neighborhoods.”

- Notorious hacker group Anonymous took credit for shutting down the city of Cleveland’s website last week, prompting an FBI investigation. Anonymous said the website was hacked in response to the police shooting of Tamir Rice, who was killed while carrying an airsoft gun.

- Spurred by the Ferguson, Missouri shooting, President Barack Obama is calling for $75 million in federal spending to get 50,000 more police to wear body cameras that record their interactions with civilians. However, Obama is not seeking to pull back federal programs that provide military-style equipment to local law enforcement.

- Drug smuggling is up at many California county jails and one reason, sheriff's officials say, is that some parolees are getting arrested just so they can try to sneak narcotics behind bars. Sheriff's departments, which run county jails, report more illegal drugs in the three years since an overhaul of the state corrections system started sending lower-level felons to county lock-ups to reduce overcrowding in state prisons. Officials say the "prison realignment" law generally has brought tougher inmates into jails and they point to a provision allowing parole violators to serve 10 days in the local jail instead of months in prison. So-called "flash incarceration," intended to give authorities a way to avoid sending parolees back to state prisons, is being used by some offenders to bring drugs, hidden inside their bodies, into county jails, sheriff’s officials say.