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
- Defense
- Law Enforcement

Turning Data into Threat Intelligence: A Case Study

Save Your Spot - October 23 Webinar

Join us on October 23 as we present a case study of how Open Source Intelligence (OSINT) can help you better protect your organization, and how you can turn data into threat intelligence faster. Note, this webinar will be hosted on the BrightTALK platform.

Top Incidents

**Energy**

- ThinkProgress.org reports that the Environmental Protection Agency announced $43 million for environmental projects on Native American grounds throughout the Southwest. According to EPA’s Regional Administrator for the Pacific Southwest Jared Blumenfeld, 44 tribes in California are in danger of running out of water. With tribes in Arizona and Nevada also suffering through extremely dry conditions, the biggest change in this year’s funding will be for more drought-specific projects. Often this involves reaching remote communities with little access to outside resources. The announcement coincided with the start of the three-day Annual Tribal/EPA Conference conference in Sacramento.
Agribusiness

- Angry over repeated cuts to their milk prices, British dairy producers continue to stage protests at their milk procurement centers, the latest coming this week at the Dairy Crest plant in Foston, England. Hundreds of dairy farmers blockaded the Dairy Crest plant in a third demonstration there over milk prices.

Insurance/Healthcare

- A federal advisory workgroup that makes privacy and security recommendations to the Office of the National Coordinator for Health IT has officially re-launched with a new name, new members, and new topics to tackle in the coming months. The Privacy and Security Workgroup, formerly known as the Privacy and Security Tiger Team, will tackle such issues as secure and private interoperability of health data and the privacy concerns related to big data.

Financial Services

- One of the largest U.S. retailers confirmed a breach that started in early September involving a "new form" of malware that infected the company's payment card systems. The breach was detected by the company's IT team on October 9th, which immediately led to a full investigation with the help of a leading IT security firm. Compromised information included debit and credit card numbers. Based on the forensic investigation to date, no personal information, debit card PINs, e-mail addresses or Social Security numbers were obtained by the hackers. The retailer also said there's no evidence that its online customers were impacted by the breach. The malware used in the attack was undetectable by current anti-virus systems.

Global Intelligence

- On 10/15/2014 Vietnam.Net, a local VNese media source, reported that the decision by Intel to invest $1 billion in its factory in Vietnam some years ago stirred up the public because of its huge investment capital. But since then, the projects capitalized at several billions of dollars have become more commonplace. According to the article, Vietnam is considering a number of huge projects valued at dozens of billions of dollars.

Legal and Regulations

- Twitter is suing the government in U.S. District Court in California, claiming that the government restrictions on the dissemination of U.S. government requests for user data violate the First Amendment. The government argues that the more is known about its sources and methods in collecting national security data, the less secure the nation will be.

Pharmaceuticals

- The Food and Drug Administration (FDA) told the US Congress yesterday it is working hard to clarify the framework for bringing experimental therapies and vaccines to patients affected by Ebola, although the agency is facing "incredible demands" as the epidemic takes hold.

Retail

- President Obama on Friday unveiled a series of steps aimed at improving the security of credit- and debit-card payments, including a pledge to shift government transactions over to the PIN and chip system and commitments from major retailers and credit card providers. In announcing the BuySecure initiative, Obama signed an executive order directing federal agencies to phase out magnetic strip credit and debit cards issued by the government, and to implement readers for the more secure PIN and chip cards in government retail locations such as national parks.

Technology
The revolution will not be televised but it will be tweeted, instant messaged or, in the case of Hong Kong, broadcast on mesh networks like FireChat. FireChat -- an "off-the-grid" smartphone app -- emerged this month as the technological glue holding Hong Kong's pro-democracy protests together and a powerful weapon in the hands of mass movements, dissidents and protesters.

**Telecommunications**

- A SSL 3.0 protocol vulnerability known as Padding Oracle On Downgraded Legacy Encryption or "POODLE" has recently been identified. This vulnerability allows a threat actor to compromise the secure connection between a user and website and steal data or launch an attack. An attacker can exploit this vulnerability to recover small amounts of plaintext from an encrypted SSL 3.0 connection by issuing crafted HTTPS requests created by client-side JavaScript code, for example.

**Defense**

- A cyberespionage team, possibly based in Russia, has been using a Windows zero day vulnerability to target a variety of organizations in several countries, including the United States, Poland, Ukraine and western Europe. The vulnerability, which will be patched today by Microsoft, is trivially exploitable and researchers say that the team behind the attacks has been using it since August to deliver the Black Energy malware. Researchers at iSIGHT Partners said that the team, which they've dubbed Sandworm, likely has been active since 2009 and has been using the Windows vulnerability CVE-2014-4114 in conjunction with a series of other flaws in order to compromise users at government agencies, NATO, academic institutions, a telecom, defense and energy firms. The attackers use highly targeted spearphishing emails in order to lure users into opening a rigged PowerPoint file that contains the exploit code for the vulnerability. Once the exploit code fires, it then downloads the Black Energy malware and begins gathering sensitive data for exfiltration.

**Law Enforcement**

- FBI Director James Comey says new encryption standards by Apple and Google will create "a black hole for law enforcement" that will help sophisticated criminals avoid detection. Comey is taking up the FBI's years-long push to expand federal surveillance law to require tech companies to include a way for law enforcement to get court ordered access to data on new devices. "The law hasn't kept pace with technology," Comey said in remarks at the Brookings Institution. "This disconnect has created a significant public safety problem. We call it 'going dark,' and what it means is this: those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism."

**Energy**

- The 9th annual Mountain Justice Fall Summit is scheduled for Oct. 24-26 on Kayford Mountain in West Virginia.

- A rally will be held on Oct. 22 to support a Texas environmental activist who interfered with pipeline construction by locking himself to construction equipment. The activist is planning to use a "necessity defense" at his trial.

- The Crush Corbett Anti-Fracking Tour will hold a rally in Bloomsburg, PA on Oct. 17.

- Last week, Greenpeace occupied an oil offshore oil rig in Italy's Sicilian Channel. Greenpeace is protesting against an Italian governmental decree that offers incentives for offshore drilling and asks Prime Minister Renzi to promote ambitious EU renewable energy targets at a meeting on the 23th and 24th of October.

- ThinkProgress.org reports that the Environmental Protection Agency announced $43
According to EPA's Regional Administrator for the Pacific Southwest Jared Blumenfeld, 44 tribes in California are in danger of running out of water. With tribes in Arizona and Nevada also suffering through extremely dry conditions, the biggest change in this year’s funding will be for more drought-specific projects. Often this involves reaching remote communities with little access to outside resources. The announcement coincided with the start of the three-day Annual Tribal/EPA Conference conference in Sacramento.

- ThinkProgress.org has also posted an article discussing a report from joint investigation from the Houston Chronicle and Houston Public Media released last month. The report asserts that the number of people who have died in Texas car crashes involving commercial vehicles has increased by more than 50 percent since the fracking boom started there in 2008.

**Agribusiness**

- In the 2013/2014 annual report released this month by Gord Miller, environmental commissioner of Ontario, the report lists several major environmental concerns, one of which is the continued use of high levels of neonicotinoid pesticides. The commissioner calls for the government of Ontario to ban these pesticides.

- A new grassroots group called The Wildfire Project aims to "train, support, and network grassroots groups to help build a broad and powerful movement for social, political, economic, and ecological justice." Further, the "prioritize groups that use direct action to fight for real wins here and now, while building power for the long battles ahead." Notable activist groups The Wildfire Project has previously trained include: Occupy Homes MN, Occupy Our Homes Atlanta, New York Students Rising, and GetEQUAL. The Wildfire Project will host it's first 'National Convening' on November 13th through 16th in Florida.

- On October 10, 2014, Sustainable Pulse reported the recently published risk assessment performed by German authorities on the use of glyphosate herbicide. The findings showed glyphosate to be safe, which has drawn criticism from the firm Testbiotech. Testbiotech released a report which described the German findings as inconclusive and untenable.

- In New Jersey, the bill AB1359 which pertains to GMO labeling requirements was sent to the State and Local Government Committee from the Assembly Consumer Affairs Committee.

- A new study was published about the safety of eating GMO's. The study, conducted by Dr. Judy Carman, from Australia finds that not enough research has been done to verify the safety of eating GMO’s. The study was led by Dr. Carman but is a collaboration of researchers from the University of Adelaide, Flinders University and the Institute of Health and Environmental Research, all based in South Australia.

- This week, the EPA approved the herbicide system of Dow Agroscience, Enlist Duo. The approval has sparked widespread outrage grassroots and activist groups across the country, spurring call campaigns, petitions, etc. The approval has been rebuked by organizations such as the Center for Food Safety (CFS) who spoke out this week, harshly criticizing the EPA's approval of the herbicide system. Andrew Kimbrell, executive director for CFS, stated that the organization will pursue all available legal options to stop the commercialization of these crops.

- Angry over repeated cuts to their milk prices, British dairy producers continue to stage protests at their milk procurement centers, the latest coming this week at the
Dairy Crest plant in Foston, England. Hundreds of dairy farmers blockaded the Dairy Crest plant in a third demonstration there over milk prices.

- Constanta, whose natural harbor on the Black Sea has welcomed ships since at least the sixth century B.C., is emerging as Europe’s biggest grain transport hub in the $4.2 billion global wheat trade.

- 5 state cattlemen’s associations representing more than 170,000 cattle breeders, producers and feeders sent a letter to Agriculture Secretary Vilsack, urging him not to issue an Order for a supplemental beef checkoff under the 1996 General Commodity Promotion, Research and Information Act. Bob McCan, National Cattlemen’s Beef Association president and Victoria, Texas, cattleman says the strong turnout of signatories to this letter demonstrate the concern across the country with the Secretary’s stated intention.

- Dairy farmers staged a protest against Iceland Foods over its decision to slash the price of a four-pint carton of milk to 89p.

---

**Insurance/Healthcare**

- The Food and Drug Administration's Suzanne Schwartz, M.D., is on a mission to debunk the myth that medical device manufacturers need FDA approval for software updates or patches to address potential vulnerabilities.

- Computer scientists at Dartmouth College have developed an app for a student's smartphone designed to monitor mental health. The so-called StudentLife app can track how much a student sleeps and whether he or she is having conversations, and getting exercise. It also asks students about their state of mind and what they've been eating. Such data could be used to see depression or dangerous stress coming before it hits too hard.

- Colorado health officials say they accidentally violated the medical privacy of about 15,000 people in a recent postcard mailing. The postcards were mailed as part of a survey sent to people receiving behavioral health services through Medicaid or the Department of Human Services’ Office of Behavioral Health.

- Apps for wearable devices that are designed to track a user's pulse rate, blood-oxygen level, or location may be leaking that personal data. Leaked data could enable account hijacking or targeted spam attacks and reveal a user's location, leading to privacy concerns, and, in a worst-case scenario, the potential for the information to be abused by extortionists or stalkers.

- Community Health Systems, Inc. (CHSI) is facing more legal action resulting from its data breach that affected 4.5 million patients, as patient Briana Brito filed a class-action lawsuit against CHSI on September 19. Brito, who was hospitalized at Alta Vista Regional Hospital in Las Vegas, which is owned by CHSI, filed the suit in the 4th Judicial District Court in San Miguel County in New Mexico. According to the suit, Brito “now faces a substantial increased risk of identity theft, if not actual identity theft” because CHSI didn’t notify patients in a timely manner.

- With the goal in mind of concentrating on growing security concerns about network-connected medical devices, the Center for Internet Security (CIS) and Medical Device Innovation, Safety and Security Consortium (MDISS) have released new resources on the subject. The CIS and MDISS Security Benchmark Mapping Guidance will offer security recommendations to both medical device manufacturers and healthcare providers in evaluating the security controls for medical devices as they evaluate products to implement.

- A federal advisory workgroup that makes privacy and security recommendations to the Office of the National Coordinator for Health IT has officially re-launched with a new
name, new members, and new topics to tackle in the coming months. The Privacy and Security Workgroup, formerly known as the Privacy and Security Tiger Team, will tackle such issues as secure and private interoperability of health data and the privacy concerns related to big data.

- The Department of Health and Human Services has appointed Lucia Savage, an attorney at insurer United Healthcare, as the new chief privacy officer of the Office of the National Coordinator for Health IT. ONC is best known for its work on guidelines for the HITECH Act’s electronic health records incentive program, but its projects are changing as HITECH funding winds down.

- While only about half of healthcare organizations have dedicated security officers, industry leaders seem to agree that C-level expertise is a must for most organizations. On a fundamental level, having top-flight technology to detect threats is helpful toward securing an environment. And some CIOs may know IT security very well. But being able to prioritize risks instantaneously and make decisions on the spot to reduce those risks requires a unique blend of talents. The challenge is finding CISOs who have both a strong set of IT security skills and healthcare acumen.

- HIPAA attorney Brad Rostolsky expects to see a ramping up of federal investigations concerning the inappropriate sale of protected health information for marketing purposes. Among the many provisions of the HIPAA Omnibus Rule, which went into effect last year, was strengthening the limitations on the use and disclosure of PHI for marketing and fundraising purposes and prohibiting the sale of PHI without individual authorization. Under the rule, patients have to opt in and provide authorization in writing for their PHI to be used for paid marketing relationships.

---

**Financial**

**Financial Services**

**Activism**

- Housing activists held a protest on October 15th and 16th in front of the corporate office of a property management company in Atlanta, GA in support of a tenant facing eviction from her rental home in Stone Mountain, GA.

- Occupy Wall Street activists and a British actor/author of a new book critical of politicians and big financial services institutions conducted a march on Tuesday, October 14th from Zuccotti Park to Wall Street. The group went on to conduct an additional anti-Wall Street event at Union Square in New York City.

- A housing activist group launched a last-minute phone campaign against the head of FHFA (the Federal Housing Finance Agency) on Tuesday, October 14th, to demand that the director of the agency force the two GSEs for housing to use principal reduction to stop foreclosures.

- A Detroit, MI-based housing activist group will organize a “mass protest” on October 22nd at the office of a real estate firm in Birmingham, MI, accusing the firm of “illegal foreclosures.”

- Housing activists will hold a solidarity action event on October 18th in Chicago, IL in support of a local homeowner facing eviction from a local lender.

- Housing activists held an anti-eviction rally on October 17th in Chicago, IL in support of a local family facing eviction by the Cook County Sherriff’s Department from their lender-owned residential property.

- Activists in UK will organize an anti-austerity protest in London on October 18th. The
activists are planning a four-day industrial strike action.

- Activists conducted a People’s Climate March in Boston, MA on October 19th to speak out against political and financial issues contributing to a climate crisis. Activists will conduct another People’s Climate March in Boston on October 22nd.

- Activists will conduct a speak-out action on October 20th at City Hall in New York City after law enforcement denied activists’ request for permits to conduct an anti-police brutality march on October 22nd from Union Square to Wall Street.

**Information Security Risk**

- Europol said criminal gangs are plotting a $1 billion (£618 million) cyber-heist on global financial institutions. Secret monitoring of internet chatrooms by the European police investigative body discovered planning by sophisticated Russian cyber-criminals aimed at “pulling off one massive hit” on a bank.

- One of the largest U.S. retailers confirmed a breach that started in early September involving a “new form” of malware that infected the company’s payment card systems. The breach was detected by the company’s IT team on October 9th, which immediately led to a full investigation with the help of a leading IT security firm. Compromised information included debit and credit card numbers. Based on the forensic investigation to date, no personal information, debit card PINs, e-mail addresses or Social Security numbers were obtained by the hackers. The retailer also said there’s no evidence that its online customers were impacted by the breach. The malware used in the attack was undetectable by current anti-virus systems.

- Hackers claimed to have hacked a popular file hosting service company and are in possession of nearly 7 million usernames (email addresses) and passwords. The hosting company however denied the claim that their systems were breached. The hackers promised to release account details in return for Bitcoin donations.

- Researchers reported that Russian hackers have exploited a bug in Microsoft’s Windows operating system in order to target computers used by NATO, the European Union, Ukraine and the telecommunications and energy sectors. The researchers said the zero-day vulnerability impacts all supported versions of Microsoft Windows and Windows Server 2008 and 2012.

- A leading security researcher warned of security issues regarding recurring video- and audio conference-based meetings that companies make available to their employees via a set of popular online conferencing tools run by a leading American technology company. These services allow customers to password-protect meetings, but, according to the researcher, it was trivial to find dozens of major companies that do not follow this basic best practice and allow virtually anyone to join daily meetings about internal discussions and planning sessions. Many of the meetings that can be found by a cursory search within an organization’s “Events Center” listing on the site seem to be intended for public viewing, such as product demonstrations and presentations for prospective customers and clients. However, from there it is often easy to discover a host of other, more proprietary meetings simply by clicking through the daily and weekly meetings listed in each organization’s “Meeting Center” section on the website.

- Researchers said a new list of targeted financial institutions has been spotted in the configuration file of Retefe malware, which now aims at banks in Japan. The Trojan is designed for man-in-the-middle (MiTM) attacks consisting of intercepting the connection from the user to the bank by changing the DNS settings, allowing the connection to be re-routed through the cybercriminal’s infrastructure. The trojan is distributed through spam campaigns. At least nine Japanese banks are targeted: Chiba Bank, Yamagata Bank, Chugoku Bank, Japan Post Bank, Awa Bank, Daishi Bank, Hokkoku Bank, Musashino Bank, and Miyazaki Bank. The researchers said previous attacks have been seen targeting banks in Switzerland, Sweden, Austria and
several other European countries.

- Hackers claimed that they intend to doxx employees and board members of an international financial institution that provides a network that enables financial institutions worldwide to send and receive information about financial transactions. The hackers also indicated they may launch a DDoS attack against a U.S. post-trade financial services company providing clearing and settlement services.

- A new survey of 257 organizations concluded that the average cost of cybercrime to a business is $7.6m per year. Actual costs range from $500,000 to $61m per company, a rise of 10% from last year's survey. The 257 companies canvassed by the survey said they experienced 429 “discernible cyber-attacks,” which equates to 1.7 successful attacks per company per week, on average. Types of cybercrime experienced by respondents, according to the survey are: viruses, worms, trojans - 98 percent; malware - 97 percent; botnets - 59 percent; web based attacks - 58 percent; phishing - 52 percent; malicious code - 51 percent; denial of service - 49 percent; stolen devices - 49 percent; malicious insiders - 35 percent.

- Reports said a website for a popular charity organization managed by the U.S. bank that recently had its 76 million customer data compromised by hackers was also infiltrated by the same group. The hackers are said to have gained access to passwords and contact information for participants.

- Researchers identified a Russian forum member offering code signing certificates issued by one of the largest CAs for sale. The forum thread was opened on a Russian password-protected forum that serves as an illegal platform for cybercrime related discussions. On the forum, one can find sales of financial malware, stolen databases and exploits, as well as technical discussions regarding hacking and programming. The post about the sale of certificates was initially published two months ago, and the topic is still being updated regularly. In the first message, the post author offered one certificate for sale in exchange for almost $1000. According to the seller, the certificate can be used to sign exe files. Forum members who are interested in purchasing are requested to connect via an instant messaging service based on XMPP protocol, highly popular among Russian cybercriminals.

- Researchers said malicious actors are using the Simple Service Discovery Protocol (SSDP) common to millions of devices using the Universal Plug and Play (UPnP) Protocol standard to launch distributed denial of service (DDoS) attacks. Armed with a list of vulnerable devices, attackers can use them as reflectors to amplify a DDoS attack against their chosen target, flooding them with bogus requests. The researchers said the prevalence of vulnerable devices is likely to lead to the further development and refinement of attack payloads and tools.

- Researchers discovered a new POS malware called ‘FrameworkPOS,’ which is a new variant of the malware that stole 56 million debit and credit card numbers from a popular home improvement chain. The new variant uses DNS requests to exfiltrate stolen data. The researchers strongly advise companies using PoS systems to have a passive DNS to store and monitor DNS activities because, if configured correctly, this can send out alerts in case suspicious behavior is detected.

- The United States Computer Emergency Readiness Team warned users to protect against email scams and cyber campaigns using the Ebola virus disease (EVD) as a theme. Phishing emails may contain links that direct users to websites which collect personal information such as login credentials, or contain malicious attachments that can infect a system. Users are encouraged to use caution when encountering these types of email messages.

- The U.S. Federal Bureau of Investigation issued a warning to companies and organizations on Wednesday, October 15th, of cyber-attacks by people linked with the Chinese government. The advisory, issued privately, is said to contain information recipients can use to help determine whether their systems have been compromised by these actors and provides steps they can take to mitigate any continuing threats. The statement said the Bureau has recently observed online intrusions that they
attribute to Chinese government affiliated actors, and private sector security firms have also identified similar intrusions.

- A new study on the Russian cybercrime scene noted that a top trend is the fact that the Russian market for stolen credit card information has become much more structured in the last year, complete with wholesalers and online trading platforms. Revenue is increasing accordingly; the report estimates that the value of the carding market has reached about $680 million. The report also said that all sampled cards were originally stolen from a popular U.S. retail chain that suffered a security breach in December of last year. The report also found that 80% of payments on a popular online card market are made using Bitcoin, with other crypto currencies also playing a role as convenient tools for illegal transactions.

Legal, Litigation, Regulatory Risk

- Global regulators announced Wednesday, October 15th, that clearing houses that help make trading derivatives safer will have to spell out how they would recover from a crisis without needing taxpayer bailouts. The final rules will be incorporated in a draft European Union law due in early 2015.

- A self-described whistleblower claimed that he is being sued by his former boss at a leading U.S. bank for content on his blog. The whistleblower requests donations to help pay for “paperwork, court fees, and countersue for damages” caused by the removal of his blogs.

- An article published last week highlighted that various lawsuits are being filed against a leading U.S. bank over “mortgage-backed securities or MBS,” and that investors are alleging that the bank has sold unwarranted MBS home loans. The author wrote that investors are asking courts to certify their suits against the “misrepresentation and faulty warranties that banks have made in its MBS sales transaction.”

Operational Risk

- Top U.S. regulators and their British counterparts conducted “war games” Monday, October 13th, to rehearse how they would handle the failure of a huge financial firm with operations in both countries. The exercise was intended to test the new strategy developed by international regulators in the past six years aimed at handling the collapse of megabanks without the taxpayer bailouts and market tumult that characterized the 2008 crisis. Making the plan work, and convincing the world it can work, was part of the regulators’ drive to end the problem of “too big to fail” institutions, those whose collapse would do so much damage to the wider economy that policy makers would be forced to use taxpayer funds to keep them in business. Monday marked the first time that various principals, or officials who would make the “big calls” in a real-life crisis, met in person for such an exercise.

- A new grassroots group is advertising its services to train, support, and network various activist groups who seek social, political, economic, and ecological justice. The group claims to have trained several activists groups already, including some groups that have a history of targeting financial firms for various perceived injustices.

Reputational Risk

- An article published last week reported that Americans are facing a “new foreclosure nightmare” because debt collectors are chasing them down for their loans. Advocates for banks say that the former homeowners ought to pay what they owe. Consumer advocates counter that “deficiency judgments” force those who have just recovered from financial collapse back into debt, and that the banks share culpability because they made the unsustainable loans in the first place.

- An article published last week said debt collectors are tracking down former homeowners owing money to mortgage lenders by freezing their bank accounts, garnishing wages, and seizing their assets. A GSE for housing was reported to be one of the most aggressive debt pursuers. The article said from January 2010 through
June 2012, the GSE allegedly referred 293,134 foreclosures out of 595,128 cases to
debt collectors.

- A Federal Reserve Governor commented that "the plethora of banking scandals"
cannot be written off as just the work of a few bad actors, that there are so many
problems in the financial industry that it cannot be considered "a few bad apples," and
that structures within the firms need to be addressed.

- An article published last week said struggling homeowners "shouldn't hold their breath
waiting for relief" from leading U.S. banks that have settled with the Department of
Justice because as anti-foreclosure and housing advocates point out, out-of-court
settlements protect banks from exposing their predatory lending practices through
evidence discovery in courts.

Global Intelligence

China

- Xinhua news service reported that Foxconn confirmed that the strike which
occurred at their Chongqing plant on Oct 9th was caused by a reduction of overtime
hours and therefore, overtime pay. Overtime hours were cut recently in an effort to
increase efficiency and decrease cost. Foxconn stated that the dispute was resolved
and workers returned to work the next day. Furthermore, factory production remained
unaffected.

- Digitimes reported that United Microelectronics Corporation (UMC) recently
reached an agreement to invest in a 12-inch fab in Xiamen, China. According to the
report, UMC will keep its advanced manufacturing processes, mainly 28/14nm
processes, in Taiwan. The new fab in Xiamen will require a total investment of up to
$6.2 billion USD and is expected to begin operations in February 2015.

- On 10/12/2014, a Chinese news outlet reports the hackers group Anonymous
attacks 52 Chinese governmental websites and obtains a number of user credentials
and information. These attacks have been considered to be a limited-scale attacks.

- On 10/12/2014, a Chinese news outlet reports 11 individuals arrested for
defacing and launching DDoS attacks against governmental websites during the
Occupy Central period in Hong Kong.

- On 10/11/2014, a Chinese news outlet reports the online gaming Steam Network
has been targeted by hackers with DDoS attacks.

- On 10/14/2014, a blog posting by Trend Micro reports Android malwares are
able to exploit SSL to hide their behavior and avoid being detected.

- On 10/13/2014, a Chinese news outlet reports certain Next Media website
experienced hackers attacks and caused Apple Daily unable to view and function
properly.

- On 10/15/2014, a page on a Chinese website contains analysis on the
Chinese-made iOS trojan, Xsser mRAT that spread through Whatsapp message.

- On 10/16/2014, a Chinese news outlet reports a Chinese hacker named
"Yxcker" provoked the hacker group Anonymous for supporting Occupy Central in
Hong Kong. After a day, the Chinese hacker website was hacked by Anonymous

Malaysia
On 10/11/2014, a Malaysian news outlet reports MTUC criticize Malaysian government decision on budget for year 2015 that it did not provide any help to low-income workers in private sector.

On 10/12/2014, MTUC reports a secret ballot on 1st and 2nd of October at Infineon located at Kulim, Malaysia. The Electronic Industry Employees Union (EIEU) has won the secret ballot for union recognition at Infineon.

On 10/11/2014, the Malaysian human right activist Charles Hector posted on its blog regarding Malaysian workers are in need of unemployment benefits.

On 10/10/2014, a Malaysian news outlet reports Malaysian government is planning to revise the Labor Acts 1955 to ensure the welfare of workers in Malaysia to be defended.

**North America**

- A major multiple services operator (MSO) is being sued by a man who claims the company got him fired from his job. Conal O'Rourke filed a lawsuit in federal court accusing the company of defamation, breach of contract and illegal disclosure of his personal information to his employer.

- On 10/10/2014 Gizmodo reported that Apple supplier GT Technology filed for bankruptcy earlier in the week and announced plans to close two of its sapphire plants in Arizona and Massachusetts. According to the article 890 people will lose their jobs.

- On 10/13/2014 the Silicon Valley Business Journal reported that drivers of Facebook's shuttle buses are strategizing with Teamsters and Google is abandoning its security contractor to hire 200 of its own guards. According to the article, allied labor advocates are by no means content with their progress within the tech companies.

- On 10/14/2014 Business Insider reported that Apple and Facebook will pay female employees up to $20,000 to help cover the cost of freezing their egg. The goal is to enable women who want to continue focusing on their careers without sacrificing their chance to have children later on.

- On 10/14/2014 Silicon Valley reported that Cisco has laid off a total of 903 workers in Silicon Valley as a part of its global restructure. Cisco announced that it will cut 6,000 positions, 8% of its global workforce.

- On 10/15/2014 Pando Daily reported that Pando has been reporting the alleged wage-fixing cartel centered on Apple, Adobe, Google, and Intel. User criticized that the punishment of the allege $3 billion wage theft is an agreement with the DOJ “that does not constitute admission by the Defendants that the law has been violated or of any issue of fact or law.” User called the US' justice system grotesque and two-tier justice system.

- On 10/15/2014 JDSupra Business Advisor reported that the U.S. Equal Employment Opportunity Commission (EEOC) filed a disability discrimination lawsuit in Wisconsin against an employer that it alleges illegally required an employee to undergo a health risk assessment and biometric test or suffer adverse consequences. Specifically, the suit alleges that the employer cancelled an employee’s medical insurance after he failed to participate in a supposedly “voluntary” health assessment and biometric testing program. The EEOC maintains that the wellness program constituted disability-related inquiries that were not sufficiently job-related and consistent with business necessity as defined by the federal Americans with Disabilities Act (ADA).

- On 10/16/2014 HR Grapevine reported that technology workers have asked an appeals court to reject a $324.5 million settlement offer from Apple, Google, Adobe, and Intel.

- On 10/21/2014 San Jose labor think tank Working Partnerships USA will release a new report detailing reforms the groups are after, pay of $15-$19/hour; paid sick days;
better health and retirement benefits; more predictable hours; more full-time work; better recruitment of underrepresented groups and strong anti-retaliation laws.

Vietnam

- On 10/10/2014 FALMI, a local VNese media source that focuses on the labor market in Ho Chi Minh City, reported that within the fourth quarter of 2014, Ho Chi Minh City has filled 60,000 jobs and has the additional labor need of 35,000 laborers. Within that number, 15% requires college degrees or higher, 14% higher education degree, 22% require high school degree, 7% skilled laborer, 7% intermediate skilled laborer, and 35% unskilled laborer.

- On 10/12/2014 Lao Dong News, a local VNese media source, reported that Altamode Vietnam, located in District 9 in Ho Chi Minh City, forced 50 workers to resign from their jobs. According to the article, the company transferred old employees, disabled employees, and non-good looking employees to factory positions. Many of these individuals did not have the physical strength to fulfill their duties in the new position and were forced to resign. 14 workers from SJ Global, District 12 in Ho Chi Minh City, were forced to resign due to intolerable and belittling actions of their manager.

- On 10/15/2014 Vietnam.Net, a local VNese media source, reported that the decision by Intel to invest $1 billion in its factory in Vietnam some years ago stirred up the public because of its huge investment capital. But since then, the projects capitalized at several billions of dollars have become more commonplace. According to the article, Vietnam is considering a number of huge projects valued at dozens of billions of dollars.

Legal and Regulations

- On September 30, 2014, California Governor Brown signed Assembly Bill 1710, which made the following changes to existing privacy and data security laws:

  1. California businesses that “maintain” personal information on state residents are now required to adopt reasonable security procedures to protect personal information (a requirement that previously only applied to businesses that own or license such data);

  2. California’s breach notification law now requires that notifying entities offer identity theft protection and mitigation services to affected individuals in certain cases; and

  3. The state’s Social Security number (SSN) protection law now prohibits the sale or advertisement for sale of such numbers, with limited exception.

- California recently passed the first state law in the nation that comprehensively addresses student privacy. The Student Online Personal Information Protection Act (“SOPIPA” or “Act”), which will become effective on January 1, 2016, applies to websites, applications and online services, prohibits the use of targeted advertising, and mandates security measures which may require the encryption of data at rest and in transit.

- On October 1 the US Food and Drug Administration (FDA) issued final guidance regarding cybersecurity for medical devices. The FDA guidelines urge device manufacturers to include safety controls on devices to prevent cyber threats and recommend manufacturers outline the necessary steps that will be taken if their devices are found to be vulnerable to breaches.

- Twitter is suing the government in U.S. District Court in California, claiming that the
government restrictions on the dissemination of U.S. government requests for user
data violate the First Amendment. The government argues that the more is known
about its sources and methods in collecting national security data, the less secure the
nation will be.

- Texas Court holds Bitcoin are securities. The U.S. District Court for the Eastern District
of Texas recently granted the SEC’s Motion for Summary Judgment, holding that the
operator of a Bitcoin Ponzi scheme who defrauded investors of over $150,000 worth of
Bitcoins was subject to SEC jurisdiction, and subsequently ordered Bitcoin Savings &
Trust (BS&T) and its founder to pay more than $40 million in disgorgement and
penalties.

Pharmaceuticals

- Lilly plans to sell one of its three plants in Puerto Rico, because the patents on
some of the drugs made there have expired.

- Some of the biggest pharmaceutical retailers in British Columbia are threatening
legal action if they are prohibited from selling tobacco products.

- The Food and Drug Administration (FDA) told the US Congress yesterday it is
working hard to clarify the framework for bringing experimental therapies and
vaccines to patients affected by Ebola, although the agency is facing “incredible
demands” as the epidemic takes hold.

Retail

- International Dairy Queen, the ice cream chain owned by Warren Buffett’s
Berkshire Hathaway Inc. (BRK/A), said customer data were compromised by
hackers. The breach with the so-called Backoff malware affected 395 of more than
4,500 U.S. locations, the unit of Omaha, Nebraska-based Berkshire said today in a
statement. The systems contained customer names, and the numbers and expiration
dates of their payment cards. Less than 600,000 cards were affected, said Dean
Peters, a spokesman for Dairy Queen. The Backoff software has been used to target
more than 1,000 businesses, according to the U.S. Secret Service.

- First via a filing with the US Securities and Exchange Commission, and then via
a press release, Sears Holding Corporation has confirmed a month-old breach that
affected POS systems at its Kmart stores. The breach was discovered on October 9
by Kmart’s Information Technology team, and the company immediately hired a
“leading IT security firm” to help in the investigation. “The investigation to date
indicates the breach started in early September. According to the security experts
Kmart has been working with, the Kmart store payment data systems were infected
with a form of malware that was undetectable by current anti-virus systems,” they
shared, and said that while they were able to quickly remove the malware, they still
believed that certain debit and credit card numbers have been compromised.

- Slate reported that Converse is accusing the companies of trademark
infringement and seeking monetary damages from 31 companies including Walmart,
Skechers, and Kmart; Converse is also pursuing a complaint with the International
Trade Commission to bar look-alike counterfeits from entering the country.

- The Washington Post reported that President Obama on Friday directed the
federal government to take the lead on improving the security of financial
transactions in the United States and announced a greater effort to work with banks
and credit card companies to strengthen identity theft protections. As part of the
effort, known as the BuySecure Initiative, to improve the nation’s financial security
standards, Obama said he will sign an executive order will require, starting next year,
that all payment cards and terminals issued by the federal government to use
chip-and-pin technology -- widely acknowledged to be more secure than the
magnetic strip used on all American credit cards.

· The Chicago Tribune reported that Walgreen Co.’s former Chief Financial Officer
  Wade Miquelon sued the drugstore operator Thursday, alleging he was defamed in
  news reports that suggested he was “personally responsible” for errors in the
  company’s earnings forecast. Miquelon alleged in the lawsuit that Chief Executive
  Officer Gregory Wasson and director Stefano Pessina, the company’s biggest
  shareholder, made false and defamatory comments about him to investors in early
  August.

· Bloomberg reported that Warren Buffet’s Berkshire Hathaway Inc. cut its stake in
  Tesco to less than 3 percent after Buffet stated that his eight-year investment was a
  “huge mistake”. According to its annual report, Tesco shares have declined 49
  percent this year.

· The Christian Science Monitor reported that Dick’s Sporting Goods CEO
  apologized to 12-year-old McKenna Peterson, who noticed that there were no female
  athletes in the company’s latest basketball catalog. Ed Stack, the CEO of Dick’s
  Sporting Goods responded to the complaint, “I’m sorry, We clearly messed up and I
  can personally guarantee that next year’s basketball catalog will prominently feature
  female athletes, as it should have this year.”

· A delayed start to the shopping season is causing consumers to postpone their
  holiday purchases until Thanksgiving weekend, according to the 2014 Holiday
  Purchase Intentions Survey from global information company The NPD Group.

· President Obama on Friday unveiled a series of steps aimed at improving the
  security of credit- and debit-card payments, including a pledge to shift government
  transactions over to the PIN and chip system and commitments from major retailers
  and credit card providers. In announcing the BuySecure initiative, Obama signed an
  executive order directing federal agencies to phase out magnetic strip credit and
  debit cards issued by the government, and to implement readers for the more secure
  PIN and chip cards in government retail locations such as national parks.

Technology

- The revolution will not be televised but it will be tweeted, instant messaged or, in the
case of Hong Kong, broadcast on mesh networks like FireChat. FireChat -- an
‘off-the-grid’ smartphone app -- emerged this month as the technological glue holding
Hong Kong’s pro-democracy protests together and a powerful weapon in the hands of
mass movements, dissidents and protesters.

Telecommunications

- A SSL 3.0 protocol vulnerability known as Padding Oracle On Downgraded Legacy
  Encryption or “POODLE” has recently been identified. This vulnerability allows a threat
actor to compromise the secure connection between a user and website and steal data
or launch an attack. An attacker can exploit this vulnerability to recover small amounts
of plaintext from an encrypted SSL 3.0 connection by issuing crafted HTTPS requests
created by client-side JavaScript code, for example.
Defense

- Several sophisticated threat groups have breached the systems of a major critical manufacturing company, the Department of Homeland Security (DHS) revealed last week in a report. According to the report, which summarizes the Industrial Control Systems Cyber Emergency Response Team's (ICS-CERT) activities in the second quarter of 2014, the attackers had access to the unnamed manufacturing organization's networks for several months.

- A cyberespionage team, possibly based in Russia, has been using a Windows zero day vulnerability to target a variety of organizations in several countries, including the United States, Poland, Ukraine and western Europe. The vulnerability, which will be patched today by Microsoft, is trivially exploitable and researchers say that the team behind the attacks has been using it since August to deliver the Black Energy malware. Researchers at iSIGHT Partners said that the team, which they've dubbed Sandworm, likely has been active since 2009 and has been using the Windows vulnerability CVE-2014-4114 in conjunction with a series of other flaws in order to compromise users at government agencies, NATO, academic institutions, a telecom, defense and energy firms. The attackers use highly targeted spearphishing emails in order to lure users into opening a rigged PowerPoint file that contains the exploit code for the vulnerability. Once the exploit code fires, it then downloads the Black Energy malware and begins gathering sensitive data for exfiltration.

- The FBI obtained information regarding a group of Chinese Government affiliated cyber actors who routinely steal high value information from US commercial and government networks through cyber espionage. These state-sponsored hackers are exceedingly stealthy and agile by comparison with the People's Liberation Army Unit 61398 ("APT1") whose activity was publicly disclosed and attributed by security researchers in February 2013.

- There are allegations that Chinese telecommunications equipment Huawei Technologies is seeking to gain access to National Security Agency computer networks this year in a failed cyberespionage attack.

- A highly advanced adversary dubbed “Hurricane Panda”, likely of Chinese origin, is targeting major infrastructure companies with a zero-day exploit.

- According to CrowdStrike, Hurricane Panda’s RAT of choice has been PlugX, “configured to use the DLL side-loading technique that has been recently popularized among Chinese adversaries.”

- Military co-operation in space and cyber were the key new elements in a report on revising the guidelines for the US-Japan security relationship. The interim report, which was published in early October, also describes "a more expansive partnership [that] would require enhanced capabilities and greater shared responsibilities".

Law Enforcement
FBI Director James Comey says new encryption standards by Apple and Google will create "a black hole for law enforcement" that will help sophisticated criminals avoid detection. Comey is taking up the FBI's years-long push to expand federal surveillance law to require tech companies to include a way for law enforcement to get court ordered access to data on new devices. "The law hasn't kept pace with technology," Comey said in remarks at the Brookings Institution. "This disconnect has created a significant public safety problem. We call it 'going dark,' and what it means is this: those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism."

Facebook wants assurances from the Drug Enforcement Administration that it's not operating any more fake profile pages as part of ongoing investigations. Facebook's chief security officer, Joe Sullivan, said in a letter last week to DEA Administrator Michele Leonhart that law enforcement agencies need to follow the same rules about being truthful on Facebook as civilian users. Those rules include a ban on lying about who you are. Sullivan's letter was in response to a New York woman's federal lawsuit claiming that a DEA agent created a fake online persona using her name and photographs stored on her cellphone. In court filings, the woman said her pictures were retrieved from her cellphone after she was arrested in July 2010 on drug charges and her cellphone seized. The woman claims that the fake page was being used by DEA agent Timothy Sinnigen to interact with "dangerous individuals he was investigating." The woman is asking for $250,000 in damages.

Advocacy groups have appealed a judge's ruling that denied them access to police records of license plate scans in Los Angeles, saying they are crucial to understanding the scope of government surveillance. The American Civil Liberties Union Foundation of Southern California and the Electronic Frontier Foundation want one week of records collected by the Los Angeles Police Department and Los Angeles County Sheriff's Department in August 2012 — an estimated 3 million scans. Superior Court Judge James Chalfant denied the request in August, saying the records are exempt from disclosure under California's open records law because they pertain to law enforcement investigations, and releasing them could violate individual privacy.

Perpetrators wearing "FBI" vests and badges around their neck tried to kidnap women in two separate incidents in Buffalo, New York. Police stopped an SUV in which the perpetrators and a victim were riding. The Buffalo News wrote that the victim believed she was being legitimately arrested after they rushed up to her, screaming "FBI, you’re wanted for questioning in a homicide" and placed handcuffs on her. Another victim escaped when the would-be kidnappers tried to force her into an SUV.

Border Patrol is considering using futuristic dog collars to improve security at the border. The U.S. government is exploring the possibility of outfitting its border-protecting canines with futuristic collars that can, for example, translate a dog's stress level through its bark and relay that data in real-time to a handler through a mobile device. CBP's canine teams are one of the agency's best tools in tracking potential terrorists or drugs.