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

REGISTER NOW FOR OUR CYBER SECURITY SUMMIT

You're invited to join us for our upcoming Cyber Security Event October 8 & 9 in Philadelphia, PA, featuring presentations on mobile application security, social media, advanced threats, corporate security, and more. Sign up now to reserve your spot and get more information!

Click Here To Learn More
Energy

- Activists who used lobster boats to block a coal shipment are planning to use the “necessity defense” at their trial. If the defense succeeds, it could have far-reaching implications for environmental actions in the United States.

Agribusiness

- The oil boom in the northern Plains “is creating a crisis for farmers whose grain shipments have been held up by a vast new movement of oil by rail,” said the New York Times. “The backlog is only going to get worse” with record crops to be harvested this fall. Farm groups say the railroads are favoring oil over grain, which the rail lines deny. North Dakota Sen Heidi Heitkamp says the backlog is a national problem because it affects food makers.

Insurance/Healthcare

- The work groups that advise the Office of the National Coordinator for Health IT on privacy and security issues are shifting gears as the ONC focuses on building an interoperable, nationwide health IT infrastructure.

Financial Services

- Multiple open source news outlets reported August 27th that Russian threat actors hacked and stole data from a leading U.S. investment bank in response to U.S. sponsored sanctions against Russia. Allegedly “gigabytes” of data were stolen, along with speculation that the data is being used to gain access to other banking institutions.

Global Intelligence

- A Chinese news outlet reports a ransomware called “ScarePackage” spreading in the United States. The ransomware are able to lock user device, display an “accusation” that the user is responsible for distributing pornography and involve in illegal activity and demand several hundreds US dollars in order to unlock the device.

Legal and Regulations

- A new Delaware law H.B. 295, signed into law on July 1, 2014 and effective January 1, 2015, provides for a private right of action in which a court may order up to triple damages in the event a business improperly destroys personal identifying information at the end of its life cycle. In addition to this private right of action, the Delaware Attorney General may file suit or bring an administrative enforcement proceeding against the offending business if it is in the public interest. This new law exempts from its coverage: banks and financial institutions that are merely subject to the Gramm-Leach-Bliley Act, but the law only exempts health insurers and health care facilities if they are subject to and in compliance with the Health Insurance Portability and Accountability Act (HIPAA), as well as credit reporting agencies if they are subject to and in compliance with the Fair Credit Reporting Act (FCRA). Companies that collect, receive, store or transmit personal identifying information of residents of the state of Delaware (or any of the 30+ states in the U.S. that now have data disposal laws on the books) should examine their data disposal policies and practices to ensure compliance with these legal requirements.

Pharmaceuticals

- FedEx was recently indicted for allegedly facilitating illegal online pharmacy sales. According to the indictment, the DEA, FDA, and members of Congress and their staffs informed FedEx that illegal Internet pharmacies were using their shipping services to distribute controlled substances, that FedEx knew its co-conspirator customers were shipping prescription drugs and were likely illegally selling controlled substances, and that FedEx identified internet pharmacy customers and subjected them to a special account credit policy that would better ensure that FedEx would receive payments due from these customers, in the event the companies were shut down as a result of their
Retail

- Google X, the company's research arm responsible for driver-less car technology, has been reportedly testing "autonomous aerial vehicles" that the company says are primarily intended for use in disaster relief, but that might eventually be used for delivery of consumer goods.

Technology

- A search warrant commanding Microsoft to turn over certain customer email data that is currently stored overseas was unfrozen late this week. The company declined to comply. In a statement, Microsoft said that it "will not be turning over the email and plans to appeal." This protest act by Microsoft, arguing that domestic warrants should not be able to command access to data stored abroad, has picked up support from other technology companies.

Telecommunications

- A recent hack set a new standard among scams in the bitcoin economy. Security researchers have found a series of incidents in which a bitcoin thief used a hijacking technique known as BGP which essentially redirected a portion of online traffic from nearly twenty ISPs. The objective was to steal raw Internet traffic and scour it for as many bitcoins as possible from users. Although each redirection lasted approximately 30 seconds, the individual was able to person the attack 22 times, and gain control of the processing power; totaling a measurable amount of $83,000.

Defense

- The business of supplying China with weapon systems, design expertise, and military-applicable technology will now take a sharp tick upwards as a result of the conflict in eastern Ukraine. Since the two European nations had a number of close ties and co-operative programs that are now severed due to Russia's intervention in Ukraine, both will be looking to China as a substitute customer to compensate for the business gained through selling to each another that they have now lost.

Law Enforcement

- Jolted by images of protesters clashing with heavily armed police officers in Missouri, President Obama has ordered a comprehensive review of the government's decade-old strategy of outfitting local police departments with military-grade body armor, mine-resistant trucks, silencers and automatic rifles, senior officials say. The New York Times reports that the review, coupled with proposed legislation and planned congressional hearings, opens the possibility for significant changes in Washington's approach to arming local law enforcement agencies.

Energy

- On Monday, August 25, 2014 two men locked their necks with bicycle U-locks to a pipeline construction truck as it was exiting a Precision pipeline storage yard. Precision Pipeline runs the pipeline storage facility hired by Enbridge to expand Line 6B. Acting to disrupt Precision Pipeline, 20-year-old Duncan Tarr and 22-year-old Dylan Ochala-Gorka, both so-called "Michigan" residents and organizers with a group called the Michigan Coalition Against Tar Sands (MICATS), demanded a halt to Enbridge’s expansion of line 6B as well as restitution for those still suffering from effects of the 2010 tar sands disaster.

- Members of the Santa Clara County Sheriff’s Office who responded to a major attack on San José’s Metcalf substation last year are now speaking out about what they call
botched decisions in the hours following the incident. They say a letter to a local congresswoman paints a picture of a well-coordinated response—but in reality—it’s far from the truth. Three members of the Santa Clara County Sheriff’s Office who responded to a major attack on a South Bay electrical substation last year recently revealed their belief that those in charge mishandled critical decisions just hours after the incident. “This was far more than vandalism,” said one of the first responders. “It was a serious attack and it was compromised from the start.” Two sheriff’s deputies asked the Investigative Unit to keep their identities hidden for fear of retaliation. They ultimately decided to speak out because, as the other deputy put it, “this is important.”

- A PG&E substation that was severely damaged by snipers in a mysterious 2013 attack was targeted by thieves early Wednesday, despite the utility’s efforts to beef up security. Sometime after midnight, someone stole construction equipment from the Metcalf electrical substation just south of San Jose. Pacific Gas and Electric Co. did not offer details on precisely what equipment was stolen or its value. The intruders who struck Wednesday appeared to be focused on theft. “This was different in the fact that no attempt was made to damage equipment or disrupt the grid,” said PG&E spokesman Brian Swanson. Although details remain sketchy, the company suggested Wednesday that “human error” allowed the thieves to succeed. Intruder detection alarms at the site sent signals to PG&E’s security operations but “were not appropriately addressed,” according to a company news release.

- Inspired by the success of the Islamic State (I.S., also known as ISIS or ISIL) in capturing and holding a huge swathe of Iraq and Syria and declaring it the kernel of an eventual global caliphate, the Nigerian Islamist terrorist group Boko Haram has shifted from hit-and-run mass killings and is now concentrating on holding territory and declaring an Islamic state.

- Activists who used lobster boats to block a coal shipment are planning to use the “necessity defense” at their trial. If the defense succeeds, it could have far-reaching implications for environmental actions in the United States.

- The environmental group Allegheny Defense Project claims that a proposed Marcellus Shale gas pipeline project under French Creek, just across the Pennsylvania border in southwestern New York, puts at risk endangered freshwater mussels in one of the nation’s most ecologically diverse waterways.

- A movement called #FloodWallStreet is calling for "Massive Coordinated Direct Actions Against Climate Profiteers" the day after the NYC Climate March, September 22. This call is specifically for NYC, but may result in actions coordinated around the country, as well.

### Agribusiness

- Grocery shoppers will pay record-level prices for beef and pork through 2015, says a University of Missouri think tank.

- The government announced a new approach to supporting dairy farmers, with enrollment to begin on Tuesday and conclude on Nov 28. The new Margin Protection Program, mandated by the 2014 farm law, will issue payments when the gap between feed costs and milk prices is narrower than the coverage level selected by a farmer. Participation is voluntary. Premiums are lowest for small farms.

- In a 149-page environmental assessment, the Agriculture Department says untoward impacts “are unlikely” from a field test of genetically engineered diamondback moths. Cornell University proposes a trial at its research farm to see if the GE moths, which are biologically altered so that female offspring die before reproducing, are effective in controlling the diamondback moth in the wild.

- Three groups petitioned the U.S. Fish and Wildlife Service to protect the monarch
butterfly under the Endangered Species Act. They say the monarch population nosedived by 90 percent in two decades due to loss of habitat and widespread planting of genetically engineered crops in the Midwest.

- The World Bank's special envoy on climate change says global warming could disrupt the food system "potentially within the next decade." Rachel Kyte, a World Bank vice president, spoke at a conference in the Australian capital of Canberra. "The challenges from waste to warming, spurred on by a growing population with a rising middle-class hunger for meat, are leading us down a dangerous path," she said in prepared remarks. "Unless we chart a new course, we will find ourselves staring volatility and disruption in the food system in the face, not in 2050, not in 2040, but potentially within the next decade."

- U.S. Magistrate Judge Barry Kurren ruled that a Kauai County ordinance that restricted plantings of biotech crops is pre-empted by state law. The ordinance was approved last year and slated to take effect this month.

- The oil boom in the northern Plains "is creating a crisis for farmers whose grain shipments have been help up by a vast new movement of oil by rail," said the New York Times. "The backlog is only going to get worse" with record crops to be harvested this fall. Farm groups say the railroads are favoring oil over grain, which the rail lines deny. North Dakota Sen Heidi Heitkamp says the backlog is a national problem because it affects food makers.

- USDA's Animal and Plant Health Inspection Service has published a rule that will allow the importation of beef from the Patagonia Region of Argentina. However, because of Argentina's struggles with foot-and-mouth disease, U.S. cattlemen are throwing a red flag, asking for a review of the call.

- Truck drivers in Argentina, the world's third-largest exporter of corn and soybeans, say theft and extortion are on the rise at the main port, Rosario.

- The latest fighting in the conflict between Russia and Ukraine could put a Black Sea port at risk. According to news reports, Ukrainian forces are taking positions around Mariupol, a city that is also home of one of the country's ports. Established in the 1600s, Mariupol has served as a port for centuries, exporting wheat and coal for centuries. Approximately 500,000 people live there.

- Container ships sailing across the northern Pacific are carrying more cargo and are setting course for British Columbia to avoid delays from a possible strike by U.S. West Coast longshoremen.

- The Environmental Protection Agency is likely to reduce the ethanol mandate, and the oil industry and its allies in Congress are mounting a full-court press against the renewable fuels industry.

- The European Commission has announced emergency measures to help the dairy sector cope with the impact of Russia's import ban.

---

**Insurance/Healthcare**

**Insurance**

- As of September 23, 2014, all HIPAA business associate agreements (BAAs) must be up to date and in line with the regulations set forth by the Omnibus Rule on September 23, 2013.

- Identity and access management is one of the most fundamental tasks healthcare organizations have to accomplish with tremendously broad operational and compliance implications - real, tangible business implications.
• Allstate Insurance Company ("Allstate") seeks to recover more than $6 million from 12 New York area defendants in its fourth insurance fraud lawsuit of 2014. Since 2003, Allstate has filed 56 fraud lawsuits in New York State seeking more than 257 million in damages.

• A federal agency is investigating whether the company Idaho hired to manage part of its Medicaid program has violated patient-privacy laws.

• Five Alabamians filed a federal class action lawsuit against CHSI on August 21 in the Northern District of Alabama. The five patients were treated at CHSI organizations such as Riverview Regional Medical Center, Gadsden Regional Medical Center, South Baldwin Regional Medical Center, and Stringfellow Memorial Hospital. The suit claims that CHSI failed "to implement and follow basic security procedures" by compromising patient names, addresses, birthdates, telephone numbers and Social Security numbers and exposed 4.5 million patients to potential identity fraud risks.

• A breach at Rouge Valley Centenary that involved the contact information of 8,300 new mothers possibly being sold by two employees to multiple Registered Education Savings Plan (RESP) companies may also have affected new mothers at Rouge Valley Health System's (RVHS) Ajax and Pickering site as well.

• The work groups that advise the Office of the National Coordinator for Health IT on privacy and security issues are shifting gears as the ONC focuses on building an interoperable, nationwide health IT infrastructure.

• The United States District Court for the Eastern District of Virginia held in Travelers Indemnity Company of America v. Portal Healthcare Solutions, LLC, No. 1:13-cv-917 (E.D. Va. Aug. 7, 2014), that online posting of patient medical information constituted "publication," whether or not it was viewed by a third party, and therefore triggered the insurer's duty to defend its insured against a class action seeking damages for breach of privacy claims.

• Newfoundland and Labrador's second largest health authority is apologizing to 52 patients for a privacy breach it blames on a botched fax number. Central Health says medical information was mistakenly faxed as an email to a 1-800 number instead of a 1-866 number. It says the faxing was part of routine auditing of doctors' billings and happened between May and August of this year.

• BioReference Laboratories, Inc., and its subsidiary CareEvolve, Inc., have reported that a security incident occurred because a test server used at CareEvolve was inadvertently configured so that it was accessible to the Internet for a brief period earlier this year. This server included records containing patient names, home addresses, telephone numbers, ages, patient/medical record numbers, dates of collection, clinical test data, dates of birth and, in 196 instances, Social Security Numbers.

• Cedars-Sinai Medical Center in Los Angeles announced an unencrypted laptop theft that may have compromised more than 500 patients' data. According to the Cedars-Sinai statement on its website, the laptop hard drive could have held protected health information (PHI) such as medical record numbers, patient identification numbers, lab testing information, treatment information and diagnostic information, as well as some patient Social Security numbers.

• The recent breach at Community Health Systems (CHS), which affected approximately 4.5 million people who had been referred to or received services from CHS-affiliated physicians, was enabled by the Heartbleed OpenSSL bug.

• The hospital records of approximately 6,500 patients were removed without authorization from the premises of Tri-City Medical Center in Oceanside on Aug. 8th. A former employee took logs from the Emergency Department of patients who had been admitted to the hospital or transferred to other facilities between Dec. 1, 2013, and May 13, 2014. The records included: patients' names, dates of birth, admitting physician, medical record number, diagnosis, and admit date and time.
A Boston judge provided a reminder this week that a healthcare organization’s and a patient’s rights to release medical records under HIPAA are very different, and a bid for a court order wouldn’t help a provider sidestep record disclosure laws.

A patient whose daughter’s data was compromised when Rady Children’s Hospital of San Diego experienced a data breach that impacted more than 20,000 patients is suing the organization.

Financial

Activism

- Occupy Wall Street will conduct a ‘Flood Wall Street’ action to occur September 22nd in New York City in which participants are urged to flood, blockade, sit-in, and shut down the institutions profiting from climate change. Financial institutions are referenced as likely targets, however specific corporate targets are not disclosed. The action is part of the ‘Beyond the March’ series of direct actions from September 17th through 24th protesting climate change.

- An anti-eviction activist group announced indications of an upcoming Halloween-themed action to occur in Los Angeles, CA sometime in late October, targeting multiple area bank brands. Event details are forthcoming.

- Activists are planning a series of protests targeting the NATO Summit in Wales, UK from September 30th through September 5th. Participants will protest against capitalism, the state, and NATO.

- A California based activist group staged an unannounced protest at a leading U.S. investment bank’s branch in San Francisco, CA on August 26th. The protest was in support of an area homeowner facing a perceived unjust eviction.

- An anti-eviction activist group organized a petition delivery campaign at a leading U.S. investment bank’s branches across the U.S. due to the bank’s recent settlement with the Department of Justice regarding homeowner relief. Participants encouraged the bank to distribute the funds to needy homeowners.

Information Security Risk

- Researchers uncovered a security hole that can be exploited to launch phishing attacks against users who make payments from their Android mobile devices. The vulnerability affects the in-app payment (IAP) SDKs for Google Wallet and Alibaba’s Alipay, China’s leading third-party online payment solution. The flaw identified by researchers is related to what’s known as an “intent,” the software mechanism in Android that allows users to coordinate the functions of different apps to achieve a certain task.

- More than 1,000 U.S. businesses to date have been affected by the same cyber-attack that hit a leading U.S. retailer in July 2014. The attacks are much more pervasive than previously reported, and hackers are pilfering the data of millions of payment cards from American consumers without companies knowing about it, according to a new Department of Homeland Security advisory released August 22nd.

- UK and European companies in industries including automotive, finance, energy and telecoms are being attacked by new Trojan malware called 'Carbon Grabber' that steals online banking password and other credentials. The malware deliberately targets ‘happy to help’ customer service professionals who may be more susceptible to its phishing emails.

- A security firm published a new survey that analyzed the main information security concerns of modern enterprises, revealing that 69% of IT professionals have to deal with phishing attacks at least once a week, with customer and financial data the main targets.
The survey also finds that seven out of 10 attacks originating from inside the network come from a malware infected machines. The survey of more than 200 US IT professionals also reveals that 60% of attacks come from malicious communication with the command and control server and more than half exploit software vulnerabilities.

- Nearly three months after the FBI, Europol and Britain's National Crime Agency launched "Operation Tovar" to successfully disrupt the botnet used to spread Gameover Zeus, the malware is making a global comeback. Multiple global security firms have observed new GoZ variants in circulation over the "past couple months." And while infection rates are much lower than before thus far, the new GoZ variants are smaller than previous Gameover Zeus campaigns to help evade detection.

- A new strain of crypto-malware is currently affecting Russian-speaking countries, with functions that allow it to steal email addresses and corresponding addresses, as well as to spread on its own to the victim's email contacts. The malware is written in a batch file and uses multiple freely available tools to carry out its dirty work. The attack vector is a Word document delivered via email, which claims to include a change in the terms of agreement of a service that needs to be reviewed before signing.

- A software and analysis firm reports that according to its analysis of 705 million lines of code as used by 1,316 enterprise applications, 70% of retail and 69% of financial services apps are vulnerable to data breaches. The firm claims a growing number of data breaches and security incidents can be directly linked to poor code quality, which can be attributed to tightening project deadlines and other factors.

- Multiple security firms report that more than half of the world's major corporations have servers that are still vulnerable to the Heartbleed flaw. Additionally, over 1,000 Heartbleed attacks occur daily.

- The Backoff malware for payment systems has been unveiled to have at least eight variants. The differences observed by security researchers relate to the installation path, registry entries and values, as well as the command and control (C&C) servers contacted for instructions. An analysis shows that the malware strains create multiple registry entries, all designed to launch the threat when the computer starts. A sign of Backoff infection is also the presence of a file in the Application Data folder, its name consisting of a set of 12 random characters, generated based on the amount of milliseconds elapsed since the start of the computer.

**Legal, Litigation, Regulatory Risk**

- Researchers state cellphone surveillance systems for law enforcement and intelligence agencies are poorly regulated and exceedingly secretive, and can easily find their way into the hands of repressive regimes. Among these tools are those that take advantage of the system that allows cellular networks to exchange records about users in order to provide adequate cellular service wherever they are, and use it to pinpoint the target's location (past and present). Privacy advocates are not only worried about governments getting their hands on these systems, but also about hackers and criminal gangs using them.

**Operational Risk**

- The Hong Kong stock exchanges, and 450 area brokerage houses, has been working closely to ensure that retail investors will be able to trade on the local stock market if a planned protest by Occupy Central blocks streets in the central business district on August 30th. Occupy Central has vowed to block streets in the financial district, where the exchange trading hall, the Hang Seng Indexes company and most brokers work. The biggest challenge for firms will be ensuring staff can work, either at their offices or elsewhere. This means that firms must have backup offices or other arrangements in case brokerage staff cannot reach their offices in Central. Brokers will also need to give their mobile and home numbers to their customers to allow investors to make inquiries or place trading orders.

- An increasing amount of activist groups are promoting the 'People's Climate March' to
occur September 17th through 24th in New York City, which calls to target institutions profiting from climate change.

- A new English-language online Al Qaeda publication recently featured a how-to article on making car bombs and suggested terror targets in the United States, including Times Square, Las Vegas casinos and night clubs, oil tankers and trains, various U.S. military targets, and a defense contractor in San Diego, CA. The publication also listed targets in the U.K. including a military academy and the stores of a department chain. The magazine calls for the stores to be hit on Friday during prayers so that Muslims won’t be affected. The timeline for bombing targets concludes with the date “201?”

**Reputational Risk**

- Multiple open source news outlets reported August 27th that Russian threat actors hacked and stole data from a leading U.S. investment bank in response to U.S. sponsored sanctions against Russia. Allegedly “gigabytes” of data were stolen, along with speculation that the data is being used to gain access to other banking institutions.

- A spoofed Twitter account leveraging a leading U.S. bank and its CEO was created on August 27th. Multiple tweets from the account were published in attempt to establish credibility however the account was terminated by August 30th before any potential brand-damaging tweets were published.

**Global Intelligence**

**China**

- According to reports, Microsoft allegedly reached a compromise on severance compensation with recently laid off Nokia China employees. The company reportedly agreed to increase annual bonus amounts and other conditions making the final severance package nearly the same as the formerly requested “N+6” standard.

- On 8/23/2014, a Chinese technology news outlet reports several online gaming servers, including RuneScape and EVE experienced distributed-denial-of-service attacks.

- On 8/24/2014, a Chinese technology news outlet reports contains a security vulnerabilities that allowed the system to make unauthorized phone calls.

- On 8/25/2014, a Chinese news outlet reports a new malware disguised as Facebook application to lure Android users to download. Once the device is infected, it is able to make unauthorized phone calls and text.

- On 8/25/2014, a Chinese news outlet reports 73% in 1000 popular free Android applications on Google Play Store contain security vulnerabilities, which users information could be stolen easily.


- On 8/26/2014, a Chinese technology news outlet reports a malware called “AdThief” targeting jailbroken iOS devices. The malware able to change application developers’ ad ID, an stealing income made by advertisement.

- On 8/25/2014, a Chinese news outlet reports the exposure of a team hacktivists, code 61419 of China Communist Cyber Army. According to the article, this team specialize in attacking Japanese network.

- On 8/26/2014, a Chinese technology website reports information regarding security vulnerability on Google Gmail Android application.

- On 8/26/2014, a Chinese technology website reports several security vulnerabilities on
TP Link TL-SC3171 IP Cameras.

- On 8/25/014, a Chinese technology website reports two security vulnerabilities on Alipay Android application.

- On 8/27/2014, a Chinese news outlet reports a malware dubbed as "Invisible Killer" targeting Android devices. The malware are able to hide its icon and disguised at an icon of a normal application. Once the device is turned on, the malware will be activated and able to eavesdrop phone calls, and steal user text messaged, call log, and other documents on the device.

- On 8/27/2014, a Chinese news outlet reports a ransomware called "ScarePackage" spreading in the United States. The ransomware are able to lock user device, display an "accusation" that the user is responsible for distributing pornography and involve in illegal activity and demand several hundreds US dollars in order to unlock the device.


- On 8/28/2014, a Chinese technology news outlet reports a Chinese security firm, 360 Security released a report regarding security on network routers and found that 90.2% of network routers consist of security vulnerabilities.

- On 8/28/2014, a Chinese news outlet reports the number of malwares increases by 2000 daily and 99% of them are targeting Android devices.

- On 8/29/2014, a Chinese website reports one of the most popular hackers forum, Hackforums.net experienced a security breached from Egyptian hacker(s).

**Germany**

- The German Federal Criminal Police Office (Bundeskriminalamt, BKA) published its annual cybercrime report. The overall numbers of related offenses increased by only one percent to 64,426 reported cases. However, crimes involving data corruption/computer sabotage increased by 18% (12,766 cases) and computer fraud by 15% (9,779). More sophisticated phishing attacks are of particular concern according to the BKA report. The overall numbers appear relatively low as the statistic only reflect reported and/or prosecuted cases. According to the BKA, investigations and research would suggest a large field of undiscovered crimes.

**India**

- The Times of India reported that HP has started laying off employees in Bangalore with the number of those who will eventually lose their jobs expected to be above 800. There were no commentaries regarding Intel in the article.

**Korea**

- On 8/25/2014 the Korea Herald reported that a civic group on 8/25/2014 called for Samsung Electronics Co. to take full responsibility and comply with an appellate court decision last week that held Samsung liable for the leukemia for two former production-line employees.

**North America**

- JDSupra Business Advisor reported that a recent decision by the 10th Circuit upheld an employer's inflexible leave policy. The court posed the question of whether an employer must allow employees more than a specified amount of sick leave or face liability under anti-discrimination laws. The court ruled, no and argued that inflexible leave policies could "serve to protect rather than threaten the rights of the disabled" by ensuring that disabled employees' requests for leaves aren't singled out for discriminatory treatment.

- On 8/26/2014 Virtual Press Office reported that Prime Healthcare Services, a CA based hospital management organization, has filed a complaint under the federal RICO statute
against SEIU, SEIU President, UHW, UHW President. The lawsuit accused SEIU of conspiring to extort, threaten and force Prime Healthcare to enter into a "neutrality agreement" that would enable SEIU to force all employees into the union regardless of employee choice.

- On 8/26/2014 the WSJ reported that blacks and Latinos make up a sizable share of low-wage workers cleaning and guarding Silicon Valley tech companies, where the technical workforces are overwhelmingly white and Asian. According to the article, blacks and Latinos account for 76% of landscape workers, 72% of janitors, and 41% of private security guards in Santa Clara county. The article quoted that Intel's US workforce is 8% Latino and 4% blacks.

- Major media companies are sponsoring the first ever CyberSEED event at the University of Connecticut from October 20-23, 2014. It will consist of a career day, panels by industry leaders and cybersecurity competitions with prizes. This event comes amidst UConn’s recent launch of its Center for Excellence for Security Innovation (CSI)

**Malaysia**

- On 8/26/2014, a Malaysian news out reports Fairchild Semiconductor is closing its plant in Penang and the workers will be laid off. Penang government announced the government organization, Invest Penang will offer job placement options to its effected employees.

- On 8/26/2014, the Malaysian human right activist named "Charles Hector" commented on his blog regarding the news report over the worker strike by Nepalese workers at a mechanical component manufacturing plant in Johor Bharu, Southern Region of Peninsular Malaysia. He claims that the news outlet exaggerate the strike for being a "riot". According to the blog, the Nepalese workers strike due to dissatisfaction with the factory’s alleged negligence in handling the health issue of a worker who died of chest problems that day and they demand assurance that the company will pay the salary of any foreigners who works with our company under a three-year contract – even if he were to pass away during that period.

- On 8/24/2014, a Malaysian news outlet reports Nepali workers of a mechanical component manufacturing plant riots due to their dissatisfaction with the factory’s alleged negligence in handling the health issue of a worker who died of chest problems that day. The plant is located in Johor Bharu, Southern Region on Peninsular Malaysia.

- On 8/26/2014, a Malaysian news outlet report the striking employees at HDD Technology in Johor, Southern Malaysia throwing rocks and burning a vehicle to protest mistreatment from the company.

- On 8/28/2014, Socialist Party of Malaysia posted a press statement of its website claimed the riot at JCY HDD Technology in Kulaijaya, Johor is due to employer provocation. The press statement contains information of employer mistreating its employees and demands of Socialist Party of Malaysia to resolve this issue.

- On 8/28/2014, a Malaysian news outlet reports the number of foreign workers arrested for torching HDD Technology building has rose to 49.

- On 8/27/2014, a Malaysian news outlet reports the workers strike at HDD Technology in Kulaijaya, Johor escalated. 800 workers of a factory here set fire to the building Tuesday night after they had stoned their employers office and burned down a car earlier in the day. Several images of the burning building have been included as attachment.

**Vietnam**
On 8/28/2014 ChaoBuoiSang.Net, a local VNese media source, reported that Microsoft has decided to relocate its Nokia production base from China to Vietnam. According to the article, the anticipated move has met with a glitch. In a document to the Ministry of Science and Technology and the Bac Ninh provincial People's Committee in mid-August, Microsoft said the process has been interrupted because the machines being used at the factory in China cannot be imported to Vietnam. Under Circular No 20 which takes effect as of September 1, the used machines and equipment will only be allowed to enter Vietnam if they have usage time of no more than five years and they are at least 80 percent brand-new. Under legal documents, dozens of Nokia's production lines could not be brought to Vietnam. If the move is successful, the number of production lines at Nokia's Bac Ninh factory would increase from six in late 2013 to 39 by the end of the year.

On 8/26/2014 VN Express, a local VNese media source, reported that Nokia has announced that plans to invest in Vietnam and has chosen a factory in Vietnam Bac Ninh as a major manufacturing base for its smartphone, in place of it's cheap models from before. Before Nokia, Samsung had invested nearly 6 billion USD. LG Electronics has also announced that it plans to invest 1.5 billion USD in Hai Phong within 10 months. Different from Samsung and Nokia, LG has not chosen smartphones as its set manufacturing product.

Legal and Regulations

A new Delaware law H.B. 295, signed into law on July 1, 2014 and effective January 1, 2015, provides for a private right of action in which a court may order up to triple damages in the event a business improperly destroys personal identifying information at the end of its life cycle. In addition to this private right of action, the Delaware Attorney General may file suit or bring an administrative enforcement proceeding against the offending business if it is in the public interest. This new law exempts from its coverage: banks and financial institutions that are merely subject to the Gramm-Leach-Bliley Act, but the law only exempts health insurers and health care facilities if they are subject to and in compliance with the Health Insurance Portability and Accountability Act (HIPAA), as well as credit reporting agencies if they are subject to and in compliance with the Fair Credit Reporting Act (FCRA). Companies that collect, receive, store or transmit personal identifying information of residents of the state of Delaware (or any of the 30+ states in the U.S. that now have data disposal laws on the books) should examine their data disposal policies and practices to ensure compliance with these legal requirements.

New gTLDs

The General Availability phase for 4 new gTLDs from the Donuts registry will begin September 3, 2014. The included extensions are: .accountants, .digital, .finance, .insure
The General Availability phase for 3 new gTLDs from the Uniregistry registry will begin September 3, 2014. The included extensions are: .audio, .hiphop, .juegos
The General Availability phase for 2 new gTLDs from the NetCologne GmbH registry will begin September 5, 2014. The included extensions are: .cologne, .koeln
The following are either in Sunrise or Landrush phase: .brussels, .vlaanderen, .cymru, .wales, .physio, .gifts, .restaurant, .sarl, .quebec, .click, .hosting, .property, .versicherung, .gent, .organic, .church, .guide, .life, .loans, .republican, and .xn--d1acj3b, a new gTLD in Russian meaning “children.”

On August 18, 2014, in Nguyen v. Barnes & Noble, Inc., the US Court of Appeals for the Ninth Circuit issued an opinion sending website owners a clear warning that the onus is on them to put users on notice of the terms of use to which they wish to bind consumers. In invalidating an agreement to arbitrate located in the Terms of Use posted on a website owned by Barnes & Noble, Inc., the Ninth Circuit provided guidance to website owners using so-called “browsewrap” agreements — where a website’s terms and conditions of use are generally posted on the website via a hyperlink at the bottom of the screen.
Healthcare

- In January 2013, the U.S. Department of Health and Human Services (HHS) announced the Health Insurance Portability and Accountability Act of 1996 (HIPAA) omnibus final rule (Final Rule) implementing a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information. HIPAA covered entities and business associates were required to comply with many of the applicable requirements of the Final Rule by September 23, 2013. In certain circumstances, covered entities may have been permitted to delay updating their Business Associate Agreements (BAAs) to comply with the new requirements. However, as of September 23, 2014, all BAAs must be compliant with the Final Rule.

- Since the Final Rule’s implementation, HHS also has released new guidance clarifying the Final Rule and proposals to future regulatory provisions, such as

  - **Mental Health:** In February 2014, HHS released guidance clarifying some of the most frequently asked questions regarding mental health information, such as disclosure of a minor’s mental health information. HHS’s guidance can be found [here](#).

  - **Laboratory Results:** In February 2014, HHS amended the Clinical Laboratory Improvement Amendments of 1988 (CLIA) regulations to allow laboratories to provide patients with access to their completed test reports upon their request, rather than requiring that patients receive test results from their physicians.

  - **National Instant Criminal Background Check System (NICS):** As part of the Obama Administration’s efforts to reduce gun violence, HHS issued a Notice of Proposed Rule Making on January 7, 2014, to remove legal barriers under HIPAA that may prevent states from reporting certain information to NICS. If adopted as drafted, the HIPAA Privacy Rule would be modified to permit certain discloses to NICS to identify persons prohibited by federal law from possessing or receiving a firearm for reasons related to mental health. Notably, several states, such as Illinois, have similar requirements in place.

Pharmaceuticals

- The U.S. Pharmacopeial Convention has joined a group campaigning to raise awareness of illegal online medicines sales.

- FedEx was recently indicted for allegedly facilitating illegal online pharmacy sales. According to the indictment, the DEA, FDA, and members of Congress and their staffs informed FedEx that illegal Internet pharmacies were using their shipping services to distribute controlled substances, that FedEx knew its co-conspirator customers were shipping prescription drugs and were likely illegally selling controlled substances, and that FedEx identified internet pharmacy customers and subjected them to a special account credit policy that would better ensure that FedEx would receive payments due from these customers, in the event the companies were shut down as a result of their illegal operations.

- Cancer patients, Americans who do have medical insurance, or who want to buy medication which have not been approved by the FDA are looking to the dark net for their medical needs. The article below remarks that one of the busiest dark net pharmacies, “Got Milk” is based in India where it is fully licensed by the Indian government.

- A new problem has emerged with the federal government’s Open Payments system, which is supposed to go live Sept. 30 and disclose payments to physicians by drug and device makers.

- A candidate Ebola vaccine could be given to healthy volunteers in the UK, The Gambia
and Mali as early as September, as part of a series of safety trials of potential vaccines aimed at preventing the disease that has killed more than 1,400 people in the current outbreak in west Africa.

Retail

- The Dalian Wanda Group, among China's largest retail real estate developers, is joining forces with two of the country's biggest e-commerce companies, Baidu and Tencent, in a partnership presumably designed to compete with Alibaba.

- Google X, the company's research arm responsible for driver-less car technology, has been reportedly testing "autonomous aerial vehicles" that the company says are primarily intended for use in disaster relief, but that might eventually be used for delivery of consumer goods.

- The US supermarket chain Market Basket has agreed to sell to a majority stake to former boss Arthur T Demoulas, ending a months-long dispute. In announcing his purchase, Mr Demoulas told workers, who had gone on strike in July to protest against his firing, "You are simply the best".

- Sonoco has signed a definitive agreement to acquire Weidenhammer Packaging Group for €286m ($383m) in cash.

- Amazon has reached an agreement to acquire Twitch Interactive, a leading live video platform for gamers. The acquisition is expected to close in the second half of 2014.

- Fast food restaurant Dairy Queen has confirmed that systems in some of their locations have been infected with malware that puts at risk credit and debit card data of customers of the retail chain.

- Home Depot is investigating a hack that possibly exposed its customer payment information. The company on Tuesday confirmed it has partnered with banks and law enforcement to look into "some unusual activity" relating to customers. Independent cybersecurity journalist Brian Krebs was the first to report this, saying "a massive new batch of stolen credit and debit cards" went for sale Tuesday in the black market online.

Technology

- The FBI and Apple said Monday they are beginning inquiries into allegations that online accounts of celebrities including Oscar-winning actress Jennifer Lawrence and model Kate Upton were hacked, after naked photos of the stars were posted online.

- A search warrant commanding Microsoft to turn over certain customer email data that is currently stored overseas was unfrozen late this week. The company declined to comply. In a statement, Microsoft said that it "will not be turning over the email and plans to appeal." This protest act by Microsoft, arguing that domestic warrants should not be able to command access to data stored abroad, has picked up support from other technology companies.

- Facebook made some changes to its algorithm. The biggest of these changes is that they are cracking down on clickbait.

- Disney applied for three UAV-related patents, indicating that drones could hold marionette or projection screens for nighttime entertainment.

- A set of classified documents published by The Intercept on Monday shows how the National Security Agency (NSA) makes more than 850 billion records about various
forms of communications available to other U.S. governmental agencies through a portal similar in look and feel to a traditional web search engine. The search tool, called ICREACH, provides access to all communications records collected under a Reagan-era executive order, known as executive order 12333, that targets foreign communication networks. The purview of 12333 has recently attracted negative attention due to the lack of oversight of its surveillance, and the lack of public information regarding its use and breadth.

- New restrictions on online billing in India may affect international e-commerce businesses, including Google Play, Amazon India, and Uber. The Reserve Bank of India (RBI) said last week that online transactions using credit cards for the purchase of items and services within India must be done through a bank within the country and be transacted in rupees. As the Indian Express explains, this may hurt online businesses, including Google Play, Amazon, and Uber, that route credit card transactions through an international payment gateway, bypassing the two-step verification required by the RBI.

- Sony’s PlayStation Network was taken down by hackers and the FBI was investigating the diversion of a flight carrying a top Sony executive amid reports of a claim that explosives were on board.

- Yahoo! Tech reported that Microsoft’s MSN Messenger, or Windows Live Messenger, will be fully retired on 10/31/2014.

- IndustriALL Global Union reported that reported that a broad coalition of campaigning organizations is calling on NXP Semiconductors to reinstate 24 trade union leaders who were allegedly fired during the CBA negotiations on 5/5/2014. The article claims that serious violations of workers’ rights are occurring on a daily basis and management refuses to take the essential step of reinstating the 24 union leaders. According to the article, Apple is a key customer of NXP and an NXP microchip will reportedly give the new iPhone 6 the capability to wirelessly pay for items like car park tickets and groceries.

- Business Insider reported that a group of about 50 protesters representing service employees who they allege are underpaid, blocked people from entering the main doors of the flagship Apple Store in San Francisco's Union Square on 8/28/2014. There were no commentaries regarding Intel in this article.

## Telecommunications

- A recent hack set a new standard among scams in the bitcoin economy. Security researchers have found a series of incidents in which a bitcoin thief used a hijacking technique known as BGP which essentially redirected a portion of online traffic from nearly twenty ISPs. The objective was to steal raw Internet traffic and scour it for as many bitcoins as possible from users. Although each redirection lasted approximately 30 seconds, the individual was able to person the attack 22 times, and gain control of the processing power; totaling a measurable amount of $83,000.

## Defense

- The Japanese government is considering a proposal to establish a fund to encourage local universities and institutes to play a more significant role in the indigenous development of military technologies.

- The business of supplying China with weapon systems, design expertise, and military-applicable technology will now take a sharp tick upwards as a result of the conflict in
eastern Ukraine. Since the two European nations had a number of close ties and co-operative programs that are now severed due to Russia's intervention in Ukraine, both will be looking to China as a substitute customer to compensate for the business gained through selling to each another that they have now lost.

- Google’s entry into the drone business brings financial and lobbying heft that should help the fledgling industry overcome technical and regulatory obstacles.

### Law Enforcement

- New York Police Commissioner William Bratton says the city is closely following developments overseas after Britain raised its terror threat level. Bratton said Friday there is "no specific credible threat" to New York City. He says the NYPD is working with the FBI Joint Terrorism Task Force to monitor any developments.

- Gunmen have shot at Los Angeles peace officers at least four times over the last eight days – a pace that has a Los Angeles County union official saying it appears to be "open season" on law enforcement, reports the L.A. Times.

- The Detroit Police Department will no longer answer to a U.S. Department of Justice overseer. One has been in place since 2003 after an investigation revealed numerous complaints of improper use of force by officers and improper treatment of witnesses. In 2000, then-Mayor Dennis Archer requested the probe after police were involved in 47 fatal shootings between 1995 and 2000, including six of unarmed suspects. Between 1994 and 2000, 19 witnesses died while being detained by the Detroit Police Department.

- Jolted by images of protesters clashing with heavily armed police officers in Missouri, President Obama has ordered a comprehensive review of the government’s decade-old strategy of outfitting local police departments with military-grade body armor, mine-resistant trucks, silencers and automatic rifles, senior officials say. The New York Times reports that the review, coupled with proposed legislation and planned congressional hearings, opens the possibility for significant changes in Washington’s approach to arming local law enforcement agencies.

- Since moving to a county-run police department, Camden, N.J., one of the nation’s poorest and most dangerous cities, has altered its culture to overcome years of mistrust. It has been 16 months since Camden took the unusual step of eliminating its police force and replacing it with a new one run by the county. Beleaguered by crime, budget cuts and bad morale, the old force had all but given up responding to some types of crimes, now the city has seen a significant drop in crime.

- The FBI is investigating who hacked and leaked nude photos of more than 100 well-known celebrities over the weekend, the Business Insider reports. The hacker exposed the nude photos and videos using the internet forum 4chan. Some of the victims, including Academy Award winner Jennifer Lawrence, sparked the FBI investigation by calling law enforcement. Some of the photos are reported to be fake.