Welcome to the Cyveillance Weekly Trends Report

Greetings from Cyveillance, the leader in open source threat intelligence. Since threat intelligence is constantly evolving, we publish this newsletter to keep our customers updated on the latest threats to various industries. Each week, we'll send you highlights from our analyst research reports. You can unsubscribe at any time. For the latest security news stories throughout the day, you can also follow us on Twitter, or to view the latest security articles from Cyveillance experts, subscribe to our blog.

In this Issue:
- Top Weekly Incidents
- Energy
- Agribusiness
- Insurance / Healthcare
- Financial Services
- Global Intelligence
- Legal and Regulations
- Pharmaceuticals
- Retail
- Technology
- Telecommunications
- Entertainment
- Defense
- Law Enforcement

Cyber Safety Awareness Training

Protect your Organization with Computer-Based Training

Are your employees the weak link in your security program? We want to help you educate your employees to keep them – and your organization – more secure.

Our computer-based cyber security training can help your employees learn how to protect your organization from the latest threats and reduce the high costs associated with incident remediation.

Top Incidents

Energy

- The environmental law organization Earthjustice filed a motion for rehearing with the Federal Energy Regulatory Commission (FERC) on behalf of Chesapeake Climate Action Network, Sierra Club, Lower Susquehanna Riverkeeper, Patuxent Riverkeeper, and Potomac Riverkeeper. The motion demands that the agency withdraw its approval of an LNG export facility proposed at Cove Point, Maryland. The filing positions the groups to sue the agency to challenge FERC’s inadequate environmental review of the project.
Agribusiness

• A coalition of foodmakers, meatpackers and allies from the agribusiness industry asked Congress to order an overhaul of U.S. country-of-origin meat-labeling rules. In a letter to lawmakers, the COOL Reform Coalition pointed to the World Trade Organization ruling against the rules on Oct 20 and said Congress should direct USDA "to rescind elements of COOL that have been determined to be non-compliant with international trade obligations." WTO said the U.S. regulations discriminated against livestock from Mexico and Canada. It was the second WTO decision since 2012 against the rules.

Insurance/Healthcare

• California Attorney General Kamala D. Harris recently released the second annual report detailing the 167 data breaches reported to the Attorney General’s office in 2013 that impacted 18.5 million Californians by putting their personal information at risk. The report is accompanied by recommendations from the Attorney General for consumers, businesses, and lawmakers on how to protect against data breaches and prevent them in the future. More than half of the 2013 breaches (53 percent) were caused by computer intrusions, such as malware and hacking. The remaining breaches resulted from physical loss or theft of laptops or other devices containing unencrypted personal information (26 percent), unintentional errors (18 percent) and intentional misuse (four percent).

Financial Services

• Hackers thought to be working for the Russian government breached the unclassified White House computer networks in recent weeks, resulting in temporary disruptions to some services while cybersecurity teams worked to contain the intrusion.

Global Intelligence

• On October 24, 2014, Good Electronics, an International network on human rights and sustainability in electronics, showed concerns on Sony Malaysia’s response to the letter from Good Electronics regarding labor violation on keeping foreign workers’ passport. Sony responded that after conducting a research, Sony could not find results of violating Malaysian law or the Sony Group Code of Conduct.

Legal and Regulations

• On October 17, 2014, President Obama signed an Executive Order designed to improve the financial cybersecurity of consumer financial transactions. The Executive Order requires the federal government to take steps to implement greater security protections for governmental payments, including government-issued payment cards, and to protect sensitive data about individuals that is collected and made available online by implementing, for example, multiple factors of authentication. In addition, federal agencies are required to assist and co-coordinate efforts to combat identity theft in conjunction with the Federal Trade Commission (FTC) and its www.identitytheft.gov website. White House Press Office – October 2014

Pharmaceuticals

• A group of security and information technology companies coordinated by Novetta released a report on an advanced persistent threat (APT) group dubbed Axiom Group that has used the Hikit malware family and other tools to target government agencies, law enforcement, aerospace, manufacturers, media, communications, pharmaceutical, energy, educational, and other institutions in the U.S. and several other countries since 2008. The researchers stated that the group originates in China and appears to choose targets in line with Chinese government policies.

Retail

• Merchant Customer Exchange (MCX) notified adopters of CurrentC, a mobile payment
app currently hosted in a trial phase, of an intrusion that revealed the email addresses of those with accounts for the testing program. The company reported that it is investigating and believes the intrusion was a result of a third-party vulnerability.

**Technology**

- The U.S. government sued AT&T Inc on Tuesday, alleging the No. 2 U.S. wireless carrier sold consumers unlimited data plans but would reduce their Internet speeds once they exceeded a certain amount of data.

**Telecommunications**

- German Telecom implemented national email routing for domestic consumers, meaning that emails between the company’s customers will not leave Germany on the way from sender to addressee. Both parties of the email exchange are required to be Telecom customers. Telecom CEO Höttges suggested earlier that transferred data should not leave Germany or Schengen countries after news related to the Snowden leaks about foreign government interference broke. However, his suggestion was met with some hesitation, as routing through third countries might at times provide cost advantages. German Telecom is offering its interested business clients that data will not leave the European Union.

**Entertainment**

- A former CBS journalist claims to have had her computer hacked and files deleted directly from her hard drive. Sharyl Attkisson explains this in her new book as she describes the incident, which occurred in 2012 while she was covering the Benghazi scandal.

**Defense**

- A sophisticated cyber espionage campaign which has been targeting the U.S and Western government agencies, but also dissents within and outside China called Axiom has been mainly targeting intelligence that benefits Chinese domestic and international policies, including snooping on dissidents; industrial espionage and stealing intellectual property. Cyber experts claims to have traced the Axiom attacks to the 2009 cyber operation against Google in China and other U.S. companies known as “Operation Aurora.” Cyber security expert from Novetta described them as “highly sophisticated and very prolific cyber espionage team.”

**Law Enforcement**

- The FBI is seeking new authority to hack into computers and spy on their users, the Guardian reports. The Justice Department is requesting that an obscure regulatory advisory board change the rules of searches and seizures. The two will meet November 5, 2014. Civil liberties groups claim the new rules would violate the first and fourth amendments and are questioning why the Justice Department is seeking the permission without public debate or congressional oversight.

**Energy**

- Texas-based Kinder Morgan has hit several Burnaby residents and two SFU professors, who have spoken out against the company’s pipeline test work on Burnaby Mountain, with a multi-million-dollar lawsuit according to the defendants’ lawyer. In court papers, the company states several citizens have obstructed and interfered with its field studies to assess the feasibility of an underground tunnel for the last leg of its proposed Edmonton-to-Burnaby pipeline. Adam Gold, Mia Nissen, Stephen Collis, Lynne Quarmby, Alan Dutton and the pipeline-opponent-citizen’s group “BROKE” were all served papers late Thursday.
Alternatives Journal has posted "5 Key Lessons from the Keystone XL Pipeline Fight". Those lessons are: Direct actions gets to goods, embrace unlikely allies, talk about climate change, support indigenous rights, & be relentless. Direct action revitalizes the activist community and creates new activists. Embracing unlikely allies suggests that activists should ally themselves with those groups of people an undesired project negatively affects. Talking about climate changes means that activists should force the issue of climate change into the legal and political discussion. Supporting indigenous rights is justified in light of the fact that many energy projects across Canada directly effect indigenous communities. The increased ability of those communities to practice their rights naturally lends itself to greater environmentalist support. The final lesson is self-explanatory.

According to Dr. Helen Caldicott an internationally known expert on the medical and environmental dangers of nuclear power, it's not safe to live on Cape Cod. During the final day of the trespassing trial of four anti-nuclear activists from the Cape, Dr. Helen Caldicott testified that it isn't simply the potential for a major nuclear meltdown at the Pilgrim Nuclear Power Station that should have people worried. Cancer-causing chemicals are constantly escaping from the reactor into the air and water, she said. "If I had young children, I would not live on the Cape," said Caldicott, a doctor who taught pediatrics at Harvard Medical School and was on staff at Children's Hospital Medical Center in Boston. "And if I was a pediatrician here, I would advise parents to leave. It's a very dangerous situation."

On October 39, 2014 protesters, calling themselves the Caretakers stopped crews from conducting pipeline survey work on Burnaby Mountain forcing the company to reassess how it will finish work needed for a National Energy Board decision. RCMP officers watched as some protesters confronted a Trans Mountain survey crew, yelling "go back to Texas," while another protester crawled under a survey crew's SUV, wrapped himself around the front tire and refused to leave.

The environmental law organization Earthjustice filed a motion for rehearing with the Federal Energy Regulatory Commission (FERC) on behalf of Chesapeake Climate Action Network, Sierra Club, Lower Susquehanna Riverkeeper, Patuxent Riverkeeper, and Potomac Riverkeeper. The motion demands that the agency withdraw its approval of an LNG export facility proposed at Cove Point, Maryland. The filing positions the groups to sue the agency to challenge FERC's inadequate environmental review of the project.

A group called Seattle Raging Grannies blockaded the entrances to the Washington Department of Ecology to protest the rise in oil train traffic through the state.

Ten activists were arrested last week at a blockade protesting a methane gas storage facility in Seneca Lake, NY.

Activist group Tar Sands Resistance will be hosting a “Day of Free Music & Resistance” in Fort Duchesne, UT. This event is affiliated with activities devoted to stopping unconventional oil production in the Uintah Basin.

Agribusiness

A coalition of foodmakers, meatpackers and allies from the agribusiness industry asked Congress to order an overhaul of U.S. country-of-origin meat-labeling rules. In a letter to lawmakers, the COOL Reform Coalition pointed to the World Trade Organization ruling against the rules on October 20, 2014 and said Congress should direct USDA "to rescind elements of COOL that have been determined to be non-compliant with international trade obligations." WTO said the U.S. regulations discriminated against livestock from Mexico and Canada. It was the second WTO decision since 2012 against the rules.
• U.S. Trade Representative Michael Froman said "we do not expect to have a final agreement" on the 12-nation Trans-Pacific Partnership trade pact during a meeting of U.S. and Asian leaders in early November.

• Syngenta says it acted responsibly in selling two strains of genetically engineered corn that are approved for cultivation in the United States although not allowed for import by China, says DTN. Syngenta, based in Switzerland, has been sued by farmers and agribusiness giant Cargill on grounds they lost sales because China has rejected cargoes that contain one of the varieties, MIR 162.

• The American Baker’s Association says a tentative U.S.-Mexico agreement to control imports of sugar from Mexico "is not good for bakers or all other users of sugar," says Baking Business. The bakers trade group said sugar growers want "a 100 percent monopoly on sugar supplies in the United States. It is a shame the federal government is such an enabler of this grab." A trade group for growers said the agreement, open for review for 30 days, would foster free and fair trade.

• One year after a pipeline rupture flooded a wheat field in northwestern North Dakota with more than 20,000 barrels of crude, Tesoro Corp. is still working around the clock cleaning up the oil spill — one of the largest to happen onshore in U.S. history.

• Rebuilding a huge swine farm in southern Minnesota where thousands of sows and piglets died in a weekend fire could take as long as a year, according to the operation’s managers. The massive blaze, which broke out Saturday afternoon at Cougar Run Farm near Truman, killed 11,000 sows and piglets, according to Pipestone System CEO Luke Minion. The cause is under investigation.

• Dairy farmers have targeted supermarket giant Morrisons in the UK in the latest protest against low milk prices. Milk producers blockaded the retailer’s distribution centre at Gadbrook Park, Cheshire, on Thursday (October 30, 2014).

• Irish farmers staged a 24-hour protest outside meat factories around the country to highlight low beef prices. The Irish Farmers’ Association (IFA) called for the protests to take place outside every meat processing plant in Ireland from 3pm on Monday (October 27, 2014) until Tuesday afternoon.

• Farms continue to be targeted by fraudsters through phone scams and fake invoices, warns Financial Fraud Action UK. Fraudsters telephoned the farmers and claimed that scammers were trying to cash cheques in their names. The farmers were told to move money into another account for safety, but these accounts were controlled by the gang.

• The international coalition of “No Patents on Seeds!” issued a report on seed patents in Europe. The coalition opposes the patenting of seeds and focuses attention on biotech companies, including Monsanto, Dupont, and Syngenta. The report from the group was issued ahead of hearings on October 27, 2014 at the European Patent Office. The coalition along with other groups have called for demonstrations outside the EPO, as the office is expected to make many critical decisions regarding seed patents in the coming months.

• According to an October 29, 2014 report from GMWatch, the EU Chief Scientist Anne Glover remarked that the Precautionary Principle should be disregarded when it comes to GMO’s. In response, Nassim Nicholas Taleb, the Distinguished Professor of Risk Engineering at New York University called Ms. Glover a “dangerous imbecile.”
The revelation that Karen DeSalvo, M.D., head of the Office of the National Coordinator for Health IT, will be retaining her leadership role at the agency even as she takes on a new position at the Department of Health and Human Services is raising new questions. Among the uncertainties is whether ONC will be able to maintain its focus and timeline for fleshing out its healthcare information systems interoperability roadmap, which, in part, addresses privacy and security issues involved in the national exchange of patient information used to make treatment decisions.

A House Committee chairman has issued a subpoena to former U.S. Chief Technology Officer Todd Park, calling on him to testify next month about the security of Obamacare's HealthCare.gov website and systems.

Health data security is not a new issue in the healthcare sector, but with health information exchanges (HIEs) springing up all over the country, facilities have to be aware of systems other than their own. In order to ensure that patient data and company information remain secure, some cybersecurity experts state that more healthcare organizations should work together to achieve common goals.

Insurance scams are far too common, often targeting seniors. While no area of insurance is immune, a lot of the fraud is happening within annuities and life insurance, with agents typically at the heart of annuity and life-insurance cons.

California Attorney General Kamala D. Harris recently released the second annual report detailing the 167 data breaches reported to the Attorney General's office in 2013 that impacted 18.5 million Californians by putting their personal information at risk. The report is accompanied by recommendations from the Attorney General for consumers, businesses, and lawmakers on how to protect against data breaches and prevent them in the future. More than half of the 2013 breaches (53 percent) were caused by computer intrusions, such as malware and hacking. The remaining breaches resulted from physical loss or theft of laptops or other devices containing unencrypted personal information (26 percent), unintentional errors (18 percent) and intentional misuse (four percent).

In an effort to keep patient information secure, more healthcare organizations are calling for health data encryption precautions. Encryption is an important aspect for stronger PHI security, and all members of a healthcare organizations must be part of the security process. The recent iHT2 research report, Answers to Healthcare Leaders' Cloud Questions, highlighted the fact that there is still a long way to go for the healthcare industry to create a completely secure environment. Moreover, it will take a concerted effort to make sure that the sector stays one or two steps ahead of the people who are after PHI.

The HITRUST Common Security Framework (CSF) is an important tool that healthcare organizations of all sizes can use in their approach to regulatory compliance and risk management. But what exactly are the basics of the CSF program, and what can facilities do to ensure that they are using CSF to the fullest?

When healthcare organizations fail to encrypt patients’ PHI, it is likely just a matter of time before a security or privacy issue arises. That is a lesson that the Arizona State Retirement System (ASRS) is currently learning the hard way.

Approximately 44,000 Arizona retirees may have had their personal data compromised in a healthcare security breach, according to the Arizona Republic. Those who were potentially affected were enrolled in the ASRS dental plans and were notified by the pension system this month.

The proliferation of healthcare cloud computing has allowed so many organizations to extend their environments, utilize more flexible resources, and empower their users. New types of cloud models have allowed the seamless transition of vast data points throughout the globe. But here is where we met one of our greatest cloud roadblocks: Compliance, regulations, and security.
As the healthcare industry quickly becomes more “connected,” the need for strong health IT security has perhaps never been more important. With EHRs and HIEs the norm, more organizations are working to improve how they can communicate across the board. With more facilities implementing EHRs and other automated systems, it’s essential for organizations to have the right tools, processes, and education put into place.

The proliferation of personal health data – and the possibility that it could fall into the wrong hands – has spurred growing concern among consumers. And those concerns have prompted New Jersey legislators to propose requiring health insurers to encrypt personal health data on all of their computers.

Can a hacker actually break through the cybersecurity platforms on current medical devices? That is the question that the US Department of Homeland Security (DHS) hopes to soon answer. The agency is reportedly investigating approximately two dozen cases of suspected cybersecurity flaws in medical devices. The worry is that cyber criminals could attempt to gain control of the devices remotely and create problems, such as instructing an infusion pump to overdose a patient with drugs or forcing a heart implant to deliver a deadly jolt of electricity.

The California Supreme Court has declined to hear appeals in data breach class action lawsuits against Sutter Health and Eisenhower Medical Center. The action lets stand previous court rulings that determined the healthcare providers were not liable for the breaches under the state’s Confidentiality of Medical Information Act because there was no proof that patients’ medical data was actually inappropriately viewed.

The Oregon Employment Department recently began notifying 851,322 people that their personal information may have been exposed when the department’s WorkSource Oregon Management Information System (WOMIS) was hacked. The information potentially exposed includes Social Security numbers, birthdates, addresses, and other data usually found on a job application.

Financial

**Financial Services**

**Activism**

- A housing activist group encouraged their supporters to flood the phone lines of a leading U.S. bank throughout the day on Monday, October 27, 2014 to stop the eviction of a local family in Chicago, IL.

- Activists will hold an anti-Trans-Pacific Partnership rally in Boulder, CO on November 7, 2014.

- OWS-affiliated activists conducted an anti-bank march throughout downtown Los Angeles, CA on October 28, 2014, stopping at several leading U.S bank branches to conduct rallies.

- A national bankers association in India held an “All India Protest Day” on October 30, 2014 demanding higher wages. The same group announced a plan to organize a series of follow-up protests starting on November 11th in all state capitals and regions across the country before the main nationwide bank employee strike on November 12, 2014. The November 11, 2014 event will be followed by relay strikes on December 2nd in the South, on December 3, 2014 in the North, December 4, 2014 in the West, and on December 5, 2014 in the Northeast.

- An anti-Wall Street event, ‘Nightmares from Wall Street’ parade occurred in NYC on October 31, 2014. A similarly themed event, ‘Ghosts of Wall Street,’ also took place the same day in several major cities throughout the country.
• A housing activist group on October 30, 2014 held an anti-foreclosure demonstration outside a foreclosure auction in Lynn, MA.

• An international activist group launched a petition campaign calling on a leading U.S. bank to follow other major U.S. financial institutions and say "no" to financing the expansion of the port at Abbot Point and the building of new coal mines in eastern Australia, as these will do "grave damage" to the Great Barrier Reef.

• Anonymous affiliates will organize world-wide protest march events on November 5th against "corruption and capitalism" in several major cities throughout the U.S., Europe, Australia, and New Zealand.

• Greek farmers and their supporters held an anti-EU protest at Syntagma Square in downtown Athens, Greece on November 1, 2014 , condemning the European Union’s new Common Agricultural Policy (CAP). Additional demonstrations will be held outside bank branches and local branches of the Hellenic Agricultural Insurance Organization (ELGA) and the Agricultural Social Security Organization (OGA). The farmers warned that demonstrations will escalate in January 2015.

• Housing activists will hold a protest at the ‘Save Your Detroit Home’ community event in Detroit, MI on November 13, 2014 . The event will be attended by representatives from the two GSEs for housing and other major U.S. banks.

• An anti-austerity demonstration occurred October 31, 2013 in downtown Montreal, Canada. Activists protested "the provincial Liberal government’s" austerity plan announced last spring, claiming that it will "rob" Quebecers of much-needed programs and services currently funded by the government.

• An anti-austerity demonstration occurred October 31, 2014 in Lisbon, Portugal. The Frente Comum, the main platform for trade unions representing Portugal’s government, protested the cuts in pensions and staff cuts, which it argued are unconstitutional.

• A survey conducted on October 21, 2014 concludes that 90% of Hong Kong protesters said they are willing to stay on the streets for more than a year in their fight with the government to heed their demands for a full democracy.

Information Security Risk

• A leading U.S. wireless provider is adding cookie-like tokens to Web requests traveling over its network. These tokens are being used to build a detailed picture of users’ interests and to help clients tailor advertisements, according to researchers and the communications company’s own documentation. While the company started piloting the service two years ago, privacy experts argue that the service is essentially tracking users and that companies paid for a fundamental service that should not be using the data for secondary purposes.

• An American sexual health product company notified their customers that an unauthorized intrusion into their databases containing payment information occurred August 3rd and lasted until August 28, 2014. The company said the hackers gained access to "account credentials, names and addresses, birth dates, phone numbers, email addresses and credit card information consisting of number, expiration date and the CVV (card verification value) code."

• An American athletic apparel and equipment company suffered a data breach, leaking payment information entered on their website by customers between June 1, 2014 and September 4, 2014.

• Researchers found a strain of malware that uses unsent Gmail drafts as a hidden location for "command and control" instructions which are particularly difficult to detect. The hacker first set up an anonymous Gmail account, then infected a computer on the target's network with malware. After gaining control of the target machine, the hacker opened their anonymous Gmail account on the victim's computer in an invisible
instance of Internet Explorer—IE allows itself to be run by Windows programs so that they can seamlessly query web pages for information, so the user has no idea a web page is even open on the computer. With the Gmail drafts folder open and hidden, the malware is programmed to use a Python script to retrieve commands and code that the hacker enters into that draft field. The malware responds with its own acknowledgments in Gmail draft form, along with the target data it’s programmed to exfiltrate from the victim’s network. All the communication is encoded to prevent it being spotted by intrusion detection or data-leak prevention. The use of a reputable web service instead of the usual IRC or HTTP protocols that hackers typically use to command their malware also helps keep the hack hidden.

- An American financial company providing commercial and residential mortgage services began notifying an unspecified number of customers that their personal information may have been accessed by hackers, after its employees were compromised by a phishing attack. In April 2014, a "targeted phishing attack" compromised some employees’ usernames and passwords. Attackers used the stolen credentials to log into some employees’ e-mail accounts, which are hosted by an unnamed, third party - from April 14 to April 16. The company warned by compromising the employees’ email accounts, the hackers would have been able to steal customer information, including Social Security numbers, bank account numbers, credit and debit card numbers, and driver's license numbers.

- Researchers said since mid-October 2014, a phishing campaign has targeted a wide variety of recipients while employing the Dyre/Dyreza banking malware. Elements of this phishing campaign vary from target to target including senders, attachments, exploits, themes, and payload(s). The Dyre banking malware specifically targets sensitive user account credentials. The malware has the ability to capture user login information and send the captured data to malicious actors. Phishing emails used in this campaign often contain a weaponized PDF attachment which attempts to exploit vulnerabilities found in unpatched versions of Adobe Reader.

- Hackers thought to be working for the Russian government breached the unclassified White House computer networks in recent weeks, resulting in temporary disruptions to some services while cybersecurity teams worked to contain the intrusion.

- Researchers said attackers are now using the cloud to steal data from the largest companies in ways that even sophisticated intrusion prevention systems cannot detect. The researchers identified a new type of attack that packages data into videos hosted on popular video sharing sites, a technique difficult to distinguish from normal user activity. Once attackers gain access to sensitive data in the company, they split the data into compressed files of identical sizes, similar to how the RAR archive format transforms a single large archive into several smaller segments. Next, they encrypt this data and wrap each compressed file with a video file. In doing so, they make the original data unreadable and further obscure it by hiding it inside a file format that typically has large file sizes. Then they upload the videos containing stolen data to a consumer video sharing site. While they’re large files, it’s not unusual for users to upload video files to these types of sites. If anyone checked, the videos would play normally on the site as well. After the videos are on the site, the attacker downloads the videos and performs the reverse operation, unpacking the data from the videos and reassembling it to arrive at the original dataset containing whatever sensitive data they sought to steal.

- California Attorney General said nearly half of the population in the state of California suffered from cyber-attacks in 2013. The attorney general said personal records of 18.5 million people in the state were at risk in 2013 due to cyber intrusions, a seven-fold increase from the previous year. The state suffered 167 breaches in 2013 at retailers, banks, healthcare providers and government entities, compared to 131 breaches in 2012, when about 2.5 million people were hit by data loss.

- Payment card transactions conducted at a ferry company in Delaware were compromised for almost a year, exposing card numbers and other information. The Delaware River and Bay Authority said it became aware of the compromise on July
30th, and immediately launched an investigation involving third-party forensics experts. Card processing systems related to food, beverage and retail sales at the ferry were infected with malware from September 20, 2013 to August 7, 2014, affecting about 60,000 transactions. Compromised information includes card numbers, cardholder names and card expiration dates. The malware used in the breach has been removed, and transactions conducted from August 8, 2014 and on have been processed securely, according to the authority.

- An American Outdoor apparel and gear company began notifying their online customers that malware found in their systems may have compromised payment card information entered into their databases between October 11, 2014 and October 17, 2014. The compromised information includes "names, email, billing and mailing addresses, order information, credit or debit card number, expiration date, and security code."

- Researchers observed a spike in Crowti, a ransomware similar to Cryptolocker that encrypts files on victims’ machines and then asks for payment to unlock them. The malware has existed for several months but it wasn’t until mid-October that the researchers noticed its biggest swell to date. The campaign infected 4000 different systems at its peak, with the bulk of those, 71 percent, confined to machines in the United States. Similar to CryptoWall, a fairly recent Cryptolocker variant, Crowti uses a valid digital signature to appear legitimate and then, once installed, demands users pay in Bitcoin to purportedly decrypt their files.

**Legal, Litigation, Regulatory Risk**

- London police arrested a suspect on charges that he participated in a series of ATM malware attacks that resulted in the theft of $2.6 million from 51 cash machines over the course of a three-day holiday weekend in May. Police said an Eastern European organized crime gang appears to be behind the 37-year-old suspect. The gang is known to have been systematically infecting and then jackpotting cash machines across the U.K., using a specially crafted, yet undisclosed malware.

- A hacker involved in the network intrusion of a leading U.K bank in November 2008, which led to $9 million in fraudulent ATM withdrawals, has been sentenced to 11 years in prison. The hacker, an Estonian national, pleaded guilty back in 2012 to conspiracy to commit wire fraud and computer intrusion, according to the U.S. Attorney’s Office for the Northern District of Georgia. In addition to his prison term, the hacker has been ordered to pay restitution totaling $8.4 million.

- An article reported that Wall Street’s self-funded regulator fined an investment banking unit of a leading U.S. bank a total of $6 million over violations of certain short-selling rules designed to prevent market manipulations. The article said that the regulator also criticized the bank’s supervisory systems and procedures for improperly allowing the allocation of fail-to-deliver positions to clients based solely on their short positions regardless of whether those clients caused or contributed to the bank’s fail-to-deliver position.

- An article reported that the settlement between the U.S. Securities and Exchange Commission and a leading U.S. bank hit a “roadblock” due to a dispute between the SEC’s commissioners over waiving a set of additional sanctions that will come into effect when the settlement is entered in court. The article highlighted that two Democratic SEC commissioners are unwilling to grant the bank’s request for a waiver while two Republicans support the relief measures.

- The family of a former breast cancer patient who died shortly after she was evicted from her home by a leading U.S. financial institution sued the bank, claiming that they caused her death.

**Operational Risk**

- An article claimed that the housing sector is not providing stimulus for economic recovery, and one of the factors is that the two GSEs for housing require lenders to
buy back loans if they default too quickly. As a result, the article argued, lenders are creating more strict underwriting rules and practices to determine if an applicant qualifies for a home mortgage.

- An article reported that some national retailers have decided to “modify” or “disable” their NFC readers to prevent customers from using a mobile payment service launched recently by a leading U.S. mobile phone maker.

- An article reported last week that big banks are demanding their law firms do more to protect sensitive information to ensure that they don’t become back doors for hackers.

**Reputational Risk**

- An article claimed that Americans are facing post-foreclosure “hell” as wages are garnished and assets are seized. The article said the two GSEs for housing are increasingly pressing borrowers to pay “whatever they still owe” on mortgages they defaulted on years ago.

- A new report released by an anti-fossil fuel activist website lists several major U.S. banks among the financial institutions that are most heavily invested in the coal industry. The report notes that 2014 was a regrettable record year for financial support extended to the top 65 coal companies. Ninety-two banks provided at least EUR 66 billion in financing the coal industry.

- An op-ed published last week claimed that the two GSEs for housing represent a potential risk for the entire financial system of America. According to the piece, the GSEs are major players in the financing of housing, and there is a danger in having so much risk concentrated in only two organizations. In addition, the piece claimed the GSEs have an unfair advantage since they can offer rates that are unavailable to other corporations.

- An article published last week claimed that although a U.S. post-trade financial services company and the SEC are tasked with catching illegal naked short selling, they are not doing an effective job of stopping such activities. The article claimed that naked short sellers, with cooperation from the buying clearing broker, the post-trade clearing company, and the SEC can actually sell “more shares than even exist.” The article concluded that the regulators and the media are in bed with the big investment banks, and the media is in the pocket of the “goons” who continue to use naked short selling to perpetrate the greatest fraud of our time.

**Global Intelligence**

**China**

- On October 27, 2014, a Chinese news outlet reported the Anti-Occupy Central’s petition page experienced security breach from hackers in Europe and America.

- On October 28, 2014, a Chinese news outlet reports a Chinese online store seller experienced a security breach. The unknown hacker change the price of an item from 980 RMB to 1 RMB. This caused the seller to received almost 3000 purchases of the item in 2 minutes.

- On October 28, 2014, a Chinese website reports a ransomware called Work.Koler spreading through text messages, luring users to open a URL and activate the malware in the process.

- On October 28, 2014, a Chinese website reports attackers exploiting Shellshock vulnerability breaching mail servers to create botnets network.

- On October 29, 2014, a Chinese technology news outlet reports a malicious
application exploiting a vulnerability on Android icons system and able to cause the device to crash.

- On October 30, 2014, a Chinese website reports FTP contains a remote execution vulnerability that affects several version of Unix system.

- On October 31, 2014, a Chinese website reports a new variant of virus targeting Android system called "Sexy Killer", disguised as adult-theme application and lure users to download.

- On October 31, 2014, a Chinese news outlet reports China Communist Cyber Army attack Taiwan's government websites in a regular basis. the article reports that Taiwan's Examination Department was attacks more than 70,000 times in October.

**Germany**

- On October 27, 2014, 24/7 Wall Street reported that some of Amazon's German workforce has called another strike. The German union Ver.di call the employees at Amazon to go on strike this week. For the first time, Amazon Germany's workers will go on day strikes simultaneously at five locations: Bad Hersfeld, Leipzig, Bavaria, Werne and Rheinberg.

**India**

- On October 31, 2014, The Times of India reported that a final settlement was reached for over 900 workers still employed at Nokia's phone manufacturing unit in Sriperumbudur on 10/30/2014, a day before the official closure of the plant. The deal gives the staff a sum slightly higher than the amount of Rs 6 lakh announced through a voluntary retirement scheme (VRS).

**Korea**

- In a October 26, 2014, Korean English language news article reports Samsung Electronics will provide compensation to everyone who developed leukemia after working at its chip and display manufacturing plants.

**Malaysia**

- On October 23, 2014, MTUC shared an article taken from a human right activist group website, Aliran.com regarding the undocumented immigrant workers in Malaysia is the sole cause of disease spread in Malaysia due to limited accessibility to medical treatment and health care.

- On October 24, 2014, Good Electronics, an International network on human rights and sustainability in electronics, showed concerns on Sony Malaysia's response to the letter from Good Electronics regarding labor violation on keeping foreign workers' passport. Sony responded that after conducting a research, Sony could not find results of violating Malaysian law or the Sony Group Code of Conduct.

- On October 28, 2014, MTUC reports the Deputy president of MTUC, as well as a member of the parliament criticized several employers for wrongfully dismissed their employees and given a statement that it is nothing wrong to held a picket if wrongfully dismissed.

- On October 28, 2014, a Malaysian news outlet report the case of dengue fever increased by 212% since January to October 18 of this year.

- In a October 28, 2014, Malaysian news article reports the burden Malaysians will be carrying next year due to implementation of Good and Services tax, rising cost of living.

- On October 29, 2014, a Malaysian news outlet reports a flash flood occurred in Penang due to river diversion and causing massive traffic jam.
North America

- In a October 23, 2014, posting on South Seattle Emerald reports 100 protesters gather at SEIU Local 6’s South Seattle office demanding a change of SEUI Local 6 leadership.

- On October 28, 2014, The Columbus Dispatch reported that a $1.1 billion Amazon data center may be coming to central Ohio.

- On October 28, 2014, The Guardian reported that labor brokers providing Indian high-tech workers to American companies have hijacked a professional visa program, creating an underground system of financial bondage by stealing wages and benefits, even suing workers who quit. According to the article, from 2000 through 2013, at least $29.7 million was illegally withheld from about 4,400 tech workers in the US on H-1B visas.

- On October 29, 2014, ZDNet reported that Microsoft officials notified another wave of employees that they are losing their jobs on 10/29/2014. The cuts of approximately 3,000 employees are believed to be largely support staff in human resources, finance, sales and marketing, and IT.

- On October 30, 2014, CBS News reported that IBM and Twitter are joining forces. Under their new partnership IBM customers will gain access to Twitter data, and the companies will develop decision-support tools for businesses. The companies will also develop applications for specific industries such as banking, retail consumer products, and transportation.

Vietnam

- On October 23, 2014, Thanh Nien News, a local VNese media source, reported that electronics companies such as LG Electronics are sparking a boom in industrial parks Vietnam as they seek alternatives to China’s rising labor costs. Kinh Bac City Development Share Holding Corp. plans to expand a facility in northern Vietnam after LG agreed to lease more land in the Trang Due park.

- In a October 26, 2014, news article reports US Assistant Secretary of State Tom Malinowski urges Vietnam to improves human rights in order to forge closer economic and security ties with the United States.

Legal and Regulations

- On October 28, 2014, the Federal Communications Commission announced that it has joined the Global Privacy Enforcement Network (“GPEN”), a network of approximately 50 privacy enforcement authorities from around the world. The FCC is the second U.S. privacy enforcement authority to join GPEN. The other U.S. member, the Federal Trade Commission, helped establish the network in 2010. The FCC’s joining of GPEN is consistent with its recently stepped-up privacy enforcement activities.

- On October 17, 2014, President Obama signed an Executive Order designed to improve the financial cybersecurity of consumer financial transactions. The Executive Order requires the federal government to take steps to implement greater security protections for governmental payments, including government-issued payment cards, and to protect sensitive data about individuals that is collected and made available online by implementing, for example, multiple factors of authentication. In addition, federal agencies are required to assist and coordinate efforts to combat identity theft in conjunction with the Federal Trade Commission (FTC) and its www.identitytheft.gov website. White House Press Office – October 2014

- A coalition of 13 alcohol producers and the World Federation of Advertisers recently released the Digital Guiding Principles (DGP), the first-ever set of global guidelines
Pharmaceuticals

- A group of security and information technology companies coordinated by Novetta released a report on an advanced persistent threat (APT) group dubbed Axiom Group that has used the Hikit malware family and other tools to target government agencies, law enforcement, aerospace, manufacturers, media, communications, pharmaceutical, energy, educational, and other institutions in the U.S. and several other countries since 2008. The researchers stated that the group originates in China and appears to choose targets in line with Chinese government policies.

- A former insider at CIGNA and medical billing company Zotec Partners made bombshell allegations of fraud and collusion in a series of lawsuits filed in federal and state courts which he has published in his newly released health care blog www.HealthFraudAlert.com.

- Johnson & Johnson may pay more than $250 million to resolve more than 1,000 lawsuits over its ASR hip implants that were excluded from a $2.5 billion settlement of similar claims last year over the device’s failure.

- The European Union is pushing for a right to intercept and seize medical product shipments in transit on the way to final importing destinations, on the grounds of suspected quality, safety and efficacy.

- India’s patent office has conceded a key demand of the pharmaceutical industry, dropping a proposed clause that would have enforced a more stringent examination of patent applications.

- French pharmaceuticals group Sanofi SA fired its chief executive Chris Viehbacher Tuesday, a day after a warning about sales of a key drug sent the company’s tumbling by 10%. The news ends a six-year reign in which the German-Canadian Viehbacher had ruffled feathers with staff and board members by trying to internationalize a company that is one of France’s most prestigious national champions.

- Sometime before the year ends, Michael McCaul (R-Tx.) plans to introduce legislation that would require drug makers to disclose their compassionate use policies, according to a congressional aide familiar with the issue. For instance, drug makers would have to inform patients when requests are denied and offer explanations, and they would also have to provide information about all requests that are received. The overarching idea is to pull the curtain back on the decision-making process, while finding a way to provide incentives to drug makers to comply. The white paper, which was submitted to the House Energy & Commerce Committee’s 21st Century Cures initiative, does not offer any suggestions for incentives, though

Retail

- American Soccer Company notified customers of ScoreSports.com October 23 that its systems were breached and customers’ personal information, including payment card data, may have been compromised between June 1 and September 4. The breach was detected on October 21, 2014 and the company has since secured its Web site payment system.

- Tesco has confirmed its accounting practices are under criminal investigation by the Serious Fraud Office (SFO). This follows an investigation by Deloitte, and called by the retailer’s new boss, Dave Lewis, which revealed last week that the retailer had
overestimated its 2014 half-year profits by £263m.

- Meijer appears to be the first member of the Merchant Customer Exchange to confirm it will accept both CurrentC, when it becomes available, and Apple Pay as forms of payment.

- Lowe’s is introducing a fleet of multilingual robots at one of its Orchard Supply Hardware stores to help out with customer service, the Wall Street Journal reports. The 5-foot-tall robots, called OSHbots, will greet customers at the door and ask them what they need, according to a video posted by Lowe’s Orchard Supply Hardware Co. store in San Jose, California, where the first robots will be located.

- Retail sales in Hong Kong have taken a hit after disruptions caused by the pro-democracy protests. And with little common ground between the students, who are demanding full universal suffrage in time for the 2017 Chief Executive elections, and the Hong Kong government, the protests could drag on for a while yet.

- The world’s largest retailer Wal-Mart is closing 30 stores in Japan, the company has announced.

- Merchant Customer Exchange (MCX) notified adopters of CurrentC, a mobile payment app currently hosted in a trial phase, of an intrusion that revealed the email addresses of those with accounts for the testing program. The company reported that it is investigating and believes the intrusion was a result of a third-party vulnerability.

---

**Technology**

- The U.S. government sued AT&T Inc on Tuesday, alleging the No. 2 U.S. wireless carrier sold consumers unlimited data plans but would reduce their Internet speeds once they exceeded a certain amount of data.

- The FCC is expected to vote on new neutrality rules in December. What those rules will entail remains a high-stakes parlor game. Out this week from the Wall Street Journal’s Gautham Nagesh was a report indicating that, similar to some plans proposed by extra-governmental individuals and groups, the FCC is considering a ‘hybrid’ approach to net neutrality.

- The latest service to become blocked in China is Viber, the free service that lets users make calls, text and share photos with friends, family and others.

- On October 29, 2014, Microsoft officials notified another wave of employees that they are losing their jobs.

- The cuts of approximately 3,000 employees today are believed to be largely support staff in human resources, finance, sales and marketing and IT. They are part of the 18,000 employees Microsoft officials said back in July that they’d be laying off over the course of a year.

- A media source coverage report that attackers have started delivering the Dridex malware with the “aid of macros placed inside innocent-looking Microsoft Word documents.” The document files allegedly contain macros to which the attackers attached complex programs written in Visual Basic for Applications (VBA). The macro is designed to download an executable file from one of several URLs and run it on the infected system,” and further highlights that the malware is “hosted on legitimate websites that have been hijacked by the attackers. Once it infects a computer, Dridex uses an XML-based configuration file to determine which websites to target. The threat communicates with its command and control (C&C) server over HTTP.

- Researchers at Ben Gurion University created a proof-of-concept malware, called the “AirHopper” malware which would allow attackers can transmit sensitive information...
from isolated computers to nearby mobile phones by using radio signals. A source describes that there are four main steps in the attack: getting the malware onto an isolated computer, installing malicious code onto more mobile phones, setting up a command and control system, and transmitting signals emanated by the isolated computer back to the attacker.

- Net Security reports that a research found that file sharing "poses a major threat to enterprise security." The article further highlights that file-sharing are "making enterprises extremely vulnerable to data loss and compliance violations. This vulnerability is heightened for regulated industries like financial services."

- Threat Post reports that Microsoft researchers have observed an increase in Crowti ransomware, similar to Cryptolocker that encrypts files on victims' machines and asks for payment to unlock them. The malware is being launched via .ZIP files that comes as an attachment in spam emails.

- A new report by mobile app analytics firm, App Annie, and mobile content and commerce association MEF, has identified Brazil, Indonesia, Mexico, Turkey and India as the next growth markets for app publishers — with rates of app downloads in these five markets growing substantially between Q3 2013 and Q3 2014.

### Telecommunications

- German Telecom implemented national email routing for domestic consumers, meaning that emails between the company's customers will not leave Germany on the way from sender to addressee. Both parties of the email exchange are required to be Telecom customers. Telecom CEO Höttges suggested earlier that transferred data should not leave Germany or Schengen countries after news related to the Snowden leaks about foreign government interference broke. However, his suggestion was met with some hesitation, as routing through third countries might at times provide cost advantages. German Telecom is offering its interested business clients that data will not leave the European Union.

### Entertainment

- A former CBS journalist claims to have had her computer hacked and files deleted directly from her hard drive. Sharyl Attkisson explains this in her new book as she describes the incident, which occurred in 2012 while she was covering the Benghazi scandal.

- Beats Music will be available on Southwest Airlines' Wi-Fi-enabled aircrafts and will offer passengers access to Apple's music streaming service. Music streaming will be accessible through the Southwest entertainment portal on personal devices and is compatible with iOS devices, as well as Android and most Web browsers.

### Defense

- A man who claimed to be a former Lockheed Martin engineer said on his deathbed that aliens are real and have visited Earth, in a now-viral video posted to YouTube. Boyd Bushman, who claimed to be a Lockheed Martin and Texas Instruments engineer, died on August 7, 2014 at the age of 78, but left behind a video with explosive claims about possible extraterrestrial life.
Four groups of Russian aircraft conducted large coordinated military maneuvers in European airspace over the Baltic, North Sea, Atlantic Ocean and Black Sea on 28 and 29 October. In total, 26 Russian military aircraft took part in the latest maneuvers, which saw interceptors scrambled by eight NATO and non-alliance nations.

Against the backdrop of ongoing disputes in the South China Sea, Indonesian Armed Forces (TNI) chief General Moeldoko has identified China’s growing military power as a factor that could destabilize Southeast Asia.

Lockheed Martin has announced an agreement to acquire US health information technology provider Systems Made Simple; the latest in a series of purchases by the defense group this year in non-military domains.

A White House National Security Council official confirmed October 29, 2014 that an unclassified portion of the White House network was the victim of an ongoing cyberattack, resulting in temporary system outages and loss of network connectivity for some users. Authorities worked to mitigate the threat and the attack did not cause any damage to White House computers or systems.

Several news media coverage regarding a cyber-espionage campaign that links to Russia cyber espionage campaign. Security firm, FireEye calls the group APT 28 and has been active for “at least six years. It tends to focus on targets that would be of interest to Russia, such as the Caucasus region with a focus on Georgia and European governments, military and security organizations.” APT28 targets its victims with spear-phishing emails and the common tools that the group attempts to install on computers include Sourface, a down loader; Evil toss, a backdoor used for running shell code and stealing credentials; and Chopstick.

A sophisticated cyber espionage campaign which has been targeting the U.S and Western government agencies, but also dissidents within and outside China called Axiom has been mainly targeting intelligence that benefits Chinese domestic and international policies, including snooping on dissidents; industrial espionage and stealing intellectual property. Cyber experts claims to have traced the Axiom attacks to the 2009 cyber operation against Google in China and other U.S. companies known as “Operation Aurora.” Cyber security expert from Novetta described them as “highly sophisticated and very prolific cyber espionage team.”

Security company Alien Vault discovered a keylogger called “ScanBox” which can attack a system without the need for installation. Several sources indicate that the malware targets Uyghurs, US think tanks, and hospitality industries and the malware uses Javascript to log keystrokes and collect system information that could later be used to exploit computers in other ways.

Several news media coverage recently reports that the common hacker groups that pose the greatest threats to cybersecurity are Deep Panda, Putter Panda, and Flying Kitten. Deep Panda is described as the most advanced Chinese cyber intrusion groups active. Putter Panda is described primarily American and European defense and aerospace industries, and finally Flying Kitten (formerly known as Ajax Security Team) which has begun targeting the defense earlier this year using spear-phishing emails and spoofed Microsoft Outlook Web Access pages to infiltrate the accounts of defense contractors. Deep Panda and Putter Panda are believed to originate from China while Flying Kitten is either an Iranian government entity or some private actor hired by the Iran’s government.

Lockheed Martin announced that it would join Northrop Grumman in protesting the US Air Force’s contract award for its next-generation ground-based radar which was awarded to Raytheon.
• The FBI is seeking new authority to hack into computers and spy on their users, the Guardian reports. The Justice Department is requesting that an obscure regulatory advisory board change the rules of searches and seizures. The two will meet Nov. 5. Civil liberties groups claim the new rules would violate the first and fourth amendments and are questioning why the Justice Department is seeking the permission without public debate or congressional oversight.

• It was reported that in 2007, the FBI mocked up a fake Associated Press story with the intention of tricking a suspect in a series of bomb threats at Lacey’s Timberline High School in Seattle to click on a link sent to his MySpace account. All this was done under the authority of a federal warrant. When the suspect clicked on the link, hidden FBI software revealed the suspect’s location to agents.

• FBI agents acted against the recommendation of an assistant U.S. attorney and impersonated repair technicians at a Las Vegas hotel to investigate online sports betting, the Associated Press reports. The agents shut off the Internet at a Las Vegas hotel to make it appears as though the computer and hardware needed to be repaired. Now defense attorneys representing some of the suspects are asking a federal judge to throw out the case because agents didn’t receive consent to examine the equipment being used by the suspects.

• The leaks from the grand jury investigating the police shooting of an unarmed 18-year-old in Ferguson, Mo., are not coming from the grand jurors themselves, officials said Thursday. The St. Louis area is tensely awaiting the grand jury’s decision, expected to be handed down in November, as to whether Ferguson Police Officer Darren Wilson should be criminally charged for fatally shooting Michael Brown on Aug. 9. The fatal shooting of 18-year-old Michael Brown by police in a St. Louis suburb has sparked violent anti-police protests and multiple nights of chaos. In recent weeks, local protesters and officials as prominent as U.S. Attorney General Eric H. Holder Jr. have been incensed over leaked information appearing in media reports, including what witnesses said in front of the grand jury, whose workings are supposed to be confidential. Those reports cited unnamed officials who had been briefed on the investigation. The details were largely favorable to Wilson’s account of the shooting, prompting a strongly worded statement last week from the U.S. Justice Department that “there seems to be an inappropriate effort to influence public opinion about this case.”