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 December Webcast
Making the Business Case for Threat Intelligence
December 17, 1 pm ET

To adequately protect company assets and ensure business continuity in the face of today's threats, organizations must be more proactive. Fortunately, many outside threats, actors and methods can be detected and studied in advance through open source Internet monitoring and intelligence analysis. In this webinar, we'll discuss how you can make a practical case for deploying threat intelligence in your organization.

Top Incidents

Energy
- Activists built a fake Keystone pipeline in front of Senator Mary Landrieu's Capital Hill home. A Democrat from Louisiana she has been pushing the Senate to approve the pipeline which has angered climate activists and Native American leaders including Rosebud Sioux who declared the Keystone XL an act of war.

Agribusiness
- President Barack Obama's executive order on immigration will indirectly affect at least 250,000 and perhaps as many as 500,000 farm workers, says Agriculture Secretary Tom Vilsack. During a tele-conference, Vilsack said "it's going to provide a bit more stability in terms of the agricultural workforce."
Insurance/Healthcare

- For the 16th consecutive year, the Department of Veterans Affairs failed its annual cybersecurity audit. The investigation sought to find out if the agency was in compliance with the Federal Information Security Management Act (FISMA).

Financial Services

- Microsoft released security updates to address a remote elevation of privilege vulnerability which exists in implementations of Kerberos KDC in Microsoft Windows. Exploitation of this vulnerability could allow a remote attacker to take control of an affected system.

Global Intelligence

- The future of DDoS attacks are expected to come from Vietnam, India, and Indonesia. Network World reports that these countries "might not have the most advanced Internet infrastructure, they do have a large number of insecure smartphones coming online, making them the big botnet sources for next year's distributed denial of service attacks." The article further highlights that the attackers motivation will initially be for "money" and due to the lack of controls many people may be using illegal copies of software which may contain malware.

Legal and Regulations

- On November 3, 2014, the Federal Financial Institutions Examination Council ("FFIEC"), an interagency body that prescribes principles and standards for the federal examination of financial institutions, released a set of general observations drawn from a cyber security examination work program ("Cybersecurity Assessment") conducted at over 500 community financial institutions during the summer of 2014. The FFIEC's report relates to both cybersecurity inherent risk and risk management practices and preparedness and includes themes and questions for management of financial institutions to consider concerning cyber security and preparedness.

Pharmaceuticals

- In a bid to make clinical trial results more widely available, the Obama administration has proposed new rules that require researchers in industry and academia to post findings of all studies funded by the federal government on a publicly available website. The move follows ongoing criticism that public health may be harmed because too many trial results remain hidden away.

Retail

- Between July and September of 2014, information security company SafeNet counted 320 reported data breaches, an increase of 25% compared to the third quarter of 2013. Those security failures exposed more than 183 million customer accounts. And the retail industry was hit hard. Retailers accounted for 31% of records stolen —57,216,390 data records—in 47 data breach incidents, or 15% of the data breach incidents. The only industry accounting for more breaches and lost records was the financial industry with 77,605,972 (42%) records.

Technology

- In a sign of discontent over divisions in Silicon Valley, drivers of Facebook shuttle buses voted Wednesday night to be represented by the Teamsters union.

Telecommunications

- FCC Chairman Tom Wheeler says that whatever final net neutrality rules the commission issues next year, will be challenged in the courts by major service providers.
Defense

- Researchers at Recorded Future studied Uroborous, Energetic Bear, and APT28, three main malware families out of Russia being used for cyberspying. Their research indicates China’s cyber-espionage motivations are based on economic objectives while Russia’s motivations are that they “want to show the world they are strong politically and that energy is incredibly important to them.” Uroborous -- the name used by G Data Software AG -- is also known as Epic Turla by Kaspersky Lab, Snake by BAE Systems, and SnakeNet, and has been around since at least 2008. Its main targets: governments, embassies, defense industry, research and education, and the pharmaceutical industry. The initial attack vector is either spear phishing emails or watering hole attacks via phony Flash player updates.

Law Enforcement

- High-flying drones have been spotted near airports and bridges in New York, prompting the FBI and Federal Aviation Administration to investigate. The drones were spotted by three pilots near commercial aircraft approaching John F. Kennedy International Airport. A helicopter pilot spotted two more drones near LaGuardia Airport. The drones are troublesome because they were flying at altitudes of 2,000 to 3,000 feet, far in excess of the 400-feet limit. They are seen as a distraction, and officials don’t know why they are in the air, causing some unease.

Energy

- An explosion occurred on an offshore oil and gas platform in the Gulf of Mexico on Thursday, killing one person and injuring three. The Bureau of Safety and Environmental Enforcement said Fieldwood Energy reported the explosion on its Echo Platform just before 3 p.m. about 12 miles off Louisiana’s coast. In a statement late Thursday, the Houston, Texas-based company said it was “an isolated incident that has been fully contained.” The company said the person who was killed was an employee of a contractor, and another contractor employee was seriously injured.

- Two environmental watchdog groups, Fresh Water Accountability Project and Food & Water Watch, filed a lawsuit Wednesday against Ohio Gov. John R. Kasich and the director of the Ohio Department of Natural Resources, claiming 23 frack waste operations were illegally authorized to operate.

- A 23-year-old Italian activist with Greenpeace suffered a broken leg after her boat was rammed by Spanish Navy vessels in a protest action against oil company Repsol in Spanish waters. The Greenpeace ship Arctic Sunrise was subsequently detained by the Spanish government.

- Activists built a fake Keystone pipeline in front of Senator Mary Landrieu’s Capital Hill home. A Democrat from Louisiana she has been pushing the Senate to approve the pipeline which has angered climate activists and Native American leaders including Rosebud Sioux who declared the Keystone XL an act of war. .

- Ten people were arrested Nov. 17 for blockading the gates of Texas-based Crestwood Midstream’s gas storage facility on the shore of New York’s Seneca Lake. This protest marks the fourth week of the “We Are Seneca Lake” campaign to stop the major expansion project at the methane gas storage facility where plans are underway to store highly pressurized, explosive gas in abandoned salt caverns on the west side of Seneca Lake.

- Russia Today reports that the House of Representatives passed a bill that would make it harder for scientists to guide the Environmental Protection Agency and easier for those with financial links to corporations to sit on the advisory panel. In a 229 – 191 vote led primarily by Republicans, the House passed legislation on Tuesday dubbed
H.R. 1422, which essentially restricts the EPA's ability to appoint scientists to its Science Advisory Board. The SAB is crucial in helping the EPA craft rules and regulations regarding pollution and public health. At the same time, the bill prohibits the EPA from listening to scientists whose peer-reviewed work has been cited in scientific discussions on whatever issue is being considered.

- Senate Democrats, by a single vote, stopped legislation that would have approved construction of the Keystone XL pipeline, one of the most fractious and expensive battles of the Obama presidency. The vote represented a victory for the environmental movement, but the fight had taken on larger dimensions as a proxy war between Republicans, who argued that the project was vital for job creation, and President Obama, who had delayed a decision on building it.

- Washington plans to sue the U.S. Department of Energy and its contractor to protect workers from hazardous vapors at the Hanford Nuclear Reservation, the nation's most polluted nuclear site, state Attorney General Bob Ferguson said Wednesday. A report last month found the Energy Department does not have an adequate system to detect whether harmful vapors are sickening workers. The report issued last month concluded that the methods used to study the vapor releases were inadequate, and the methods did not account for short but intense releases of vapors from the tanks. The report was prepared by a team of experts led by the Department of Energy's Savannah River National Laboratory.

- Thursday was the most dramatic day in a months-long battle between citizens and Texas-based Kinder Morgan over the company's controversial Trans Mountain pipeline expansion project. In a rapid sweep, RCMP arrested as many as two dozen Kinder Morgan protesters on Burnaby Mountain, stirring strong emotions among opponents to the Edmonton-to-Burnaby pipeline. The arrests were for "civil contempt" of a court order permitting the company's pipeline survey work.

**Agribusiness**

- President Barack Obama's executive order on immigration will indirectly affect at least 250,000 and perhaps as many as 500,000 farm workers, says Agriculture Secretary Tom Vilsack. During a tele-conference, Vilsack said "It's going to provide a bit more stability in terms of the agricultural workforce."

- In the wake of the European Parliament's vote to strengthen countries' ability to reject GMO cultivation for themselves, Bulgarian and German officials voiced strong opposition to the cultivation of GM crops. Bulgarian Foreign Minister Daniel Mitov reiterated Bulgaria's opposition to GM crops being grown and sold in the European market. German Farm Minister Christian Schmidt said "social-economic reasons" should be factored into allowing states to choose to prohibit the cultivation of GMO's.

- As voting tallies continue, the margin between "yes" and "no" votes continues to shrink. While most media outlets called the GMO-labeling bill failing early, it now appears likely that after the counting is completed, there will be a recount, with the margin falling within the 3,000 votes that trigger an automatic recount. Counties officially have until Monday at 5pm PST to finish counting votes, though it may be done ahead of time.

- Musician Neil Young's boycott of Starbucks over involvement in the lawsuits regarding Vermont's GMO-labeling legislation has been gaining traction on social media. Many posts from activist groups on Facebook are attracting followers to his cause in supporting GMO-labeling legislation.

- Two farm operations in southwestern Oregon filed suit in state court against a voter-approved ban on genetically engineered crops in Jackson County, says the Medford Mail Tribune. The farmers ask for the ban to be voided as a violation of the state's
right-to-farm law or for the court to order the county to pay them $4.2 million to compensate for lost income because they would have to destroy fields of the Roundup Ready alfalfa to comply with the ordinance. The ban, approved by a 2-to-1 margin in May, takes effect on June 6, 2015.

- ADM, the world’s largest corn processor, sued Syngenta in state court in Louisiana over cargoes of corn rejected by China because they contained an unapproved Syngenta variety. The lawsuit, which requests monetary damages, says Syngenta failed to undertake responsible stewardship to prevent its genetically engineered corn from becoming mixed with the rest of the U.S. corn supply. Cargill also is suing Syngenta over its shipments that were rejected by China for the same reason. Syngenta says the lawsuits are without merit.

- At the Agriculture Department, "more than 100 undercover agents pose as food stamp recipients at thousands of neighborhood stores to spot suspicious vendors and fraud," says the New York Times in a story about a significant expansion throughout the government of undercover work. It says at least 40 federal agencies have undercover units. In another description of USDA's undercover work, the Times said the agents "root out illegal food stamp transactions by individuals and businesses or any financial fraud involving USDA programs."

- BNSF Railway Co., the railroad owned by Warren Buffett’s Berkshire Hathaway Inc., plans to spend a record $6 billion next year to help speed trains and improve service crimped by surging grain and oil shipments.

---

**Insurance/Healthcare**

- As we all know, HealthCare.gov has had its struggles this past year. The health insurance exchange website, which is operated by the federal government under President Obama’s Affordable Care Act, was hacked at least 16 times shortly after its launch in October of 2013. Additionally, it was discovered in July of this year that a hacker had successfully uploaded malicious software to HealthCare.gov with the intention of using its systems for staging cyber-attacks against other websites. Turkey’s Council of State has ruled that biometric registration of patients must stop as it is unconstitutional. The body made the decision in response to lawsuits raised against scanning patient’s palms by the Turkish Physicians Association and other groups.

- Combating fraud and maintaining the privacy and security of health information are among the most significant management challenges facing the Department of Health and Human Services, its watchdog agency says.

- For the 16th consecutive year, the Department of Veterans Affairs failed its annual cybersecurity audit. The investigation sought to find out if the agency was in compliance with the Federal Information Security Management Act (FISMA).

- The VA inspector general (IG) will not release the full audit details until next year. However, VA Chief Information Officer Stephen Warren presented the audit results at a House Veterans Affairs Committee hearing.

- As technology continues to evolve, and healthcare organizations implement more connected options, it only makes sense that providers are working to strengthen their health data security. With tools such as patient portals and secure messaging, patients can also become more involved in their health and how their protected health information (PHI) is used and transported. However a recent survey indicates that patients may not be overly concerned about their health data security.

- A widespread auto insurance fraud investigation that spanned the state of California has now resulted in the arrest of 54 people in the Bay Area after an alleged rash of
falsified claims were submitted to insurers. The majority of the insurance claims were made by people who had previously been uninsured or underinsured, but who had then purchased coverage or added to their policies after having experienced damage to their vehicles or after having been involved in a collision.

- A former CFO at a now-shuttered hospital has pleaded guilty to submitting false documents so the medical center could receive $785,000 in payments under the HITECH Act electronic health records financial incentive program. Some legal experts predict that more federal prosecutions of HITECH Act fraud under the EHR "meaningful use" program are likely.

- The Interoperability Workgroup (IWG) formed a strategic relationship with Healthcare Information and Management Systems Society (HIMSS) and Integrating the Healthcare Enterprise (IHE) USA to improve the connectivity building process between EHR and HIE systems. The partnership will be part of IWG’s current program that tests and certifies EHRs and HIE vendors to enable reliable transfer of data within and across organizational and state boundaries. Additionally, ICSA Labs was selected to be the testing and certification body for the groups.

- A second state court ruling in recent weeks calls attention to how incidents involving alleged patient privacy violations can lead to negligence lawsuits that invoke HIPAA as a benchmark. In the most recent case, the Indiana appellate court has upheld a $1.4 million jury verdict awarded in 2013 to a customer that alleged her privacy was violated by a Walgreens pharmacist who inappropriately reviewed and shared the woman's prescription history with a third party.

- Healthcare IT security administrators can also have a difficult time when it comes to ensuring that HIPAA physical safeguards are always followed. As technology continues to evolve, so does the healthcare industry. Laptops, tablets and cell phones are quickly becoming commonplace within healthcare organizations, as doctors and nurses can use the devices to quickly communicate to one another in a secure matter. However, lost, misplaced, and stolen portable devices are one of the leading causes in healthcare security breaches. Physical safeguards are a critical aspect of healthcare organizations, especially with items being stolen from either facilities or unauthorized employees' cars.

- The U.S. Federal Trade Commission is seeking assurances from Apple Inc. that it will prevent sensitive health data collected by its upcoming smartwatch and other mobile devices from being used without owners’ consent. Apple representatives have met on multiple occasions with agency officials in recent months to stress that it will not sell its users’ health data to third-party entities such as marketers or allow third-party developers to do so.

**Financial**

**Financial Services**

**Activism**

- An activist group held a protest outside a leading U.S. bank branch in Seattle, WA on November 20, 2014, accusing the bank of “fraud and forgery” used to evict tenants from their homes. The protesters demanded that the bank return a home to a local family and pay damages for their pain, suffering, and humiliation.

- A housing activist group held a rally in Toronto, Canada on November 21, 2014 to promote and raise awareness on the right to housing.

- A new petition launched against a leading U.S. bank aims to close the bank’s ATMs in the Memphis, TN area because it will allegedly hurt local residents in attracting new
businesses to their area and “alienate prospective residents.”

- An anti-eviction activist group held a court solidarity protest on November 21, 2014 in support of a local family facing eviction in Chicago, IL.

- A petition was issued demanding an open and public Federal Joint Congressional Investigation Hearing and Testimony into several financial firms, including an American post-trade financial services company, for their role in federal income tax evasion and securities fraud stemming from the 2008 mortgage crisis.

- A prominent hacktivist collective is organizing physical protests to occur at all Federal Reserve Buildings across 13 cities on December 23, 2014 starting at 12:00pm local times. December 23, 2014 marks the Federal Reserve’s 101st birth date.

- A rally to raise the minimum wage to $15 per hour occurred November 19, 2014 in Philadelphia, PA.

- An international student movement launched a global week of action against student debt November 17 through 22, 2014 which also called for equal access to education, regardless of socioeconomic status. The campaign was primarily educational, discussion based and without physical disruptions.

**Information Security Risk**

- Hackers targeted an array of Mexican financial institutions, including the country’s central bank, under the flags of #OpRevolucion and #Ayotzinapa.

- A Russian hacker alleged to have hacked over 8,000 accounts of a leading U.S. bank. The hacker encouraged interested parties to reach out to him to purchase customer information.

- Microsoft will end support for the Windows Server 2003 operating system on July 14, 2015. After this date, this product will no longer receive: security patches that help protect PCs from harmful viruses, spyware, and other malicious software; assisted technical support from Microsoft; software and content updates.

- Microsoft released security updates to address a remote elevation of privilege vulnerability which exists in implementations of Kerberos KDC in Microsoft Windows. Exploitation of this vulnerability could allow a remote attacker to take control of an affected system.

- Drupal released an advisory to address multiple vulnerabilities in Drupal core 6.x versions prior to 6.34 and Drupal core 7.x versions prior to 7.34, one of which could allow a remote attacker to cause a denial of service. Drupal is a back-end framework for at least 2.1% of all web sites worldwide, ranging from personal blogs to corporate, political, and government sites including WhiteHouse.gov and data.gov.uk. It is also used for knowledge management and business collaboration.

- An attack that exploits the Shellshock vulnerability recently patched in the Bash Unix platform delivers a malware program that tries to compromise systems running BusyBox, a collection of Unix utilities typically used on embedded devices like routers. The backdoor-type malware is dubbed Bashlite and infects Linux-based systems through Shellshock attack vectors. After it infects a system, Bashlite malware scans the network for systems that accept Telnet connections and attempts to log in using common usernames and password combinations: root, admin, support, 12345, 123456, pass, password and toor. It then issues a series of commands to determine if the system runs BusyBox and uses it to download two remote scripts called bin.sh and bin2.sh.

- Criminals are exploiting a vulnerability in ATMs that requires no hacking software or gear. Unlike the machines deployed at brick-and-mortar bank locations, kiosk ATMs could be placed into a privileged “operator mode” simply by pressing a special sequence of buttons on the ATM keypad. From that mode, an attacker could...
manipulate a number of variables, one of which sets the denomination of the bills loaded into the machine’s currency cartridges.

- China’s censorship apparatus blocked access to a leading U.K. bank’s online corporate banking portal, affecting countless businesses in the world’s second largest economy. A report suggested that the disruption to corporate customers of the world’s second largest bank is a result of the censors trying to block access to a Content Delivery Network (CDN) provider, which it uses as part of the secure log-in system for clients. China is currently trying to take down CDN sites because they provide users inside the Great Firewall with a means to view blocked contents such as news websites and web portals.

- A mobile security firm uncovered a sophisticated piece of smartphone malware that could infect entire corporate networks if just one device is compromised. The malware is called NotCompatible and is capable of stealing data while advanced detection techniques make it much harder for traditional security measures to spot. NotCompatible gives attackers remote access to protected networks through any connected mobile device, including corporate Wi-Fi and VPNs. At its heart, NotCompatible.C is an unrestricted proxy on a mobile device that offers the operators unfettered access to protected networks to which these devices connect. An infected smartphone present on an enterprise network would potentially allow attackers to enumerate vulnerable hosts inside the network, exploit vulnerabilities in these hosts and exfiltrate data. NotCompatible targets Android smartphones and tablets.

- A new report released on November 18, 2014, concluded that Vietnam, India and Indonesia will likely be the big botnet sources for DDoS attacks in 2015 because they have a large number of insecure smartphones coming online that are more susceptible to phishing and other compromising attacks. In 2014, however, China was the single biggest source of DDOS attacks, the report said, followed by the United States and Russia.

- A local bank in Green Bay, WI suffered a data breach losing debit card details of an unspecified number of its customers.

- The Bank of England is leading a Simulated Targeted Attack and Response (STAR) initiative to occur in the next few months that invites hackers to try to penetrate the cyber defenses of Britain’s major banks and steal information about millions of customers. STAR is part of the Bank of England’s new cyber security framework called CBEST that it rolled out in June, which includes sharing intelligence from government agencies such as Britain’s GCHQ with companies, and encouraging more intense testing of financial institutions. Britain’s biggest banks are among more than 30 financial firms lining up to go through the STAR test.

- A postal inspector said on November 19, 2014 that compensation files for U.S. Postal Service workers might also have been breached during a recent hack that exposed the Social Security numbers and other personal data on about 800,000 USPS employees. Postal officials said they did not know until November 4th that any files holding employee personal information had been copied. In total, 100 machines were penetrated, out of the agency’s 25,000 servers and 200,000 workstations. The employee data affected potentially includes names, dates of birth, Social Security numbers, physical addresses, employment start dates and termination dates, emergency contacts and other personal information.

- The head of the City of London police warned that Western financial institutions should prepare themselves for cyber-attacks from Islamic militants. The Commissioner urged for preparations to be made during a security conference in New York, while suggesting that the Islamic State of Iraq and the Levant (aka ISIS) is a potential attacker. The City of London force and New York District Attorney’s Office will be stationing permanent staff in each others offices to build greater co-operation between police and prosecutors that cover the Square Mile and Wall Street. The exchange program is designed to ward off attacks.
A national office supply retail store confirmed on November 18, 2014 that its retail point-of-sale systems were compromised earlier this year by malware-wielding attackers. The store declined to say how many of its more than 2,000 stores in 26 countries - including 1,800 across the United States and Canada - may have been affected by the breaches.

Cyber criminals started targeting the password managers that protect an individual’s most sensitive credentials by using a keylogger to steal the master password in certain cases. Researchers found that a configuration file, which attackers use to tailor the Citadel trojan for specific campaigns, had been modified to start up a keylogger when the user opens either Password Safe or KeePass, two open-source password managers. While malware has previously targeted the credentials stored in the password managers included in popular web browsers, third-party password managers have typically not been targeted.

**Legal, Litigation, Regulatory Risk**

- The U.S. Supreme Court has agreed to hear cases brought by a leading U.S. bank questioning whether a second mortgage on an underwater house can be voided during bankruptcy.

- The Federal Reserve will meet with regulators and several leading U.S. banks to discuss the development of a reference rate alternative to LIBOR.

- Two Democratic members of Congress sent letters to 16 financial institutions seeking information about any data breaches they've experienced and detailed briefings from corporate IT security officers as the House and Senate consider cyber security legislation. Among the information being sought: a description of all data breaches the organization has experienced; the approximate number of customers that may have been affected and how they were notified of the breach; the findings from forensic investigative analyses or reports; the individuals or entities suspected or believed to have caused the data breaches; a description of data protection improvement measures the organization is taking; an estimate of the number and value of fraudulent transactions that were connected to the data breaches; a description of the data security policies and procedures involving vendors, third-party service providers and subcontractors; and any recommendations for improvements in cyber security laws.

- A leading U.S. investment firm fired two employees for leaking confidential information from the Federal Reserve Bank of New York, raising questions about the bank’s alleged close relationship with its regulator. The bank said a junior employee was terminated for passing on to a colleague information from the New York Fed, his former employer, while a supervisor was fired for knowing about the matter but not escalating it.

- European police announced 15 arrests designed to stem the use of remote-access Trojans. Such malware has been tied to hundreds of thousands of infections worldwide. The anti-RAT operation was led by French police, coordinated by Europol’s European Cybercrime Center, and resulted in arrests across Estonia, France, Italy, Latvia, Norway, Romania and the United Kingdom. Criminals who successfully deploy RATs can gain complete control over target computers, wherever they are in the world. Police officials say attackers often tap such tools to spy on women or girls via webcams, access consumers’ banking and other personal details, commit extortion, as well as turn machines into launch pads for distributed-denial-of-service attacks.

**Operational Risk**

- An article published by a leading East Coast newspaper reported the Housing and Urban Development Secretary indicated eliminating the two GSEs for housing will be a priority for the Obama administration in the next congress. The Housing secretary allegedly stated that there was bipartisan support for “doing away” with the GSEs and replacing them with a new system for housing finance.
The price of 38 companies' stock encountered technical problems that caused their shares to stop updating on a NYC-based stock exchange for almost half hour on November 17, 2014, from 10:22am EDT to 10:46am. The exchange described the glitch as a problem that occurs when a stock is in “a locked [and] crossed state.” That is one in which a stock’s bid and ask price are the same.

The SEC voted unanimously on November 19, 2014 in favor of regulations designed to ensure the technology at stock exchanges works. The Commission voted to adopt rules on Regulation Systems Compliance and Integrity (Reg SCI), which requires self-regulatory organizations, securities exchanges, registered clearing agencies and significant alternative trading systems, to establish policies and procedures to help ensure that systems have capacity, integrity and resiliency. Proponents however voiced concern that Reg SCI excludes broker dealers and many alternative trading centers that trade equities and fixed income securities.

The CEO of a prominent online retailer continues to criticize Wall Street and current stock market activity as a corrupt operation, promoting cryptocurrencies such as Bitcoins as a means to circumvent current corrupt financial markets.

**Reputational Risk**

- An article reported that a data sharing scheme which has involved U.S. financial institutions helping New York prosecutors uncover human trafficking cases is to be extended to Europe. The article claimed the partnership has involved many leading U.S. banks as well as money-transfer companies, highlighting suspicious transactions to law enforcement agencies.

- A post argued that deficiency judgments shouldn’t be allowed when the foreclosure that created the deficiency was performed using “robo-signed fraudulent documents.” The post also said that the erroneous assumption is that GSEs for housing are “justified” in pursuing deficiencies from former borrowers; however, they do not loan money to borrowers and there is no justification for the GSEs to pursue anyone in that regard.

- An article reported that a leading U.S. bank is advocating for net-neutrality “behind closed doors.”

- A new survey on banks’ customer service shows that credit unions ranked highest while mega-banks ranked worst.

- A consumer accused a leading U.S. bank of conspiring with a major online lending exchange to deliberately and deceptively hide consumer disclosures in its loan generation practices, calling to boycott both companies.

---

**Global Intelligence**

**China**

- A Chinese website reports 360 Security came across a malicious Trojan disguised as a flashlight application for mobile devices.

- A Chinese technology news outlet reports that Android Lollipop contains a high risk security vulnerability that could be exploited to send out any broadcast.

- A Chinese news outlet reports Baidu Mobile Guard discovered a new malware dubbed as "Dark Lurker,” which has infected 30 million mobile devices.

- A Chinese news outlet reports that the three suspects for creating and spreading "Wirelurker", a malicious application targeting Apple system have been arrested.
• A Chinese news outlet reports the number of cyber attacks in India have increased by five times over the past three years, with most of the attacks are originated from Chinese.

• A Chinese news outlet reports an individual has been arrested for stealing Japanese Apple users’ Appstore credit through online games, forums, and QQ Qun(group).

• A Chinese news outlet reports that the China Communist Cyber Army launched more than 7 millions cyber attacks on Taiwan's National Security Bureau over the past year, but none of the attacks were successful. According to the article, the China Communist Cyber Army not only launched attacks against Taiwan's government websites, but also researched different kinds of malwares, hacking mobile devices to obtain sensitive information.

• Digtimes reported that the recent free trade agreement (FTA) consensus between China and South Korea will have an impact on Taiwan's competitive advantage and weigh on foreign investments in Taiwan in various industries such as flat panels, petrochemical, iron and steel, machine tools, glass and automotive.

• Timesunion.com reported that Chinese censors are blocking access to several popular websites as China prepares to host the World Internet Conference, a gathering of the world top technology companies.

• A Chinese news outlets reported that employees at Xianda Electronics factory in Zhaoqing, Guangdong Province went on strike mainly due to wages in arrears. Workers reportedly demonstrated with protest banners and pleaded local government to intervene on the workers’ behalf. Zhaoqing Xianda Electronics is wholly-owned by US-based panel supplier, OCULAR, and mainly produces LCD displays.

Europe

• Members of the European parliament are said to have drafted a motion which calls for “unbundling [of] search engines from other commercial services”, according to the Financial Times. The motion, said to be voted on next week, is supported by German, French, and Spanish politicians and is seen as part of the antitrust case Google faces in the EU, even though Google is not mentioned by name in the resolution draft. The antitrust case is another dimension to Google’s challenges in Europe after this year’s decision by the European Court of Justice regarding the “Right to be Forgotten”. The authority to actually force a break-up of search engines and other services is questionable, both in respect to the jurisdiction between the EU Parliament and EU Commission, as to the EU’s authority to regulate the US business.

India

• Technical support scammers in India are maligning a technical support company that asserts a partnership with Microsoft. The firm--called SB3--outsources its work to India but does not actually partner with Microsoft.

Israel

• The Globes reported that Histadrut chairman Nissenkorn declared a general labor dispute in Israel on 11/18/2014. The Histadrut says that the grounds for the dispute are the low wage, the increasing use of contract workers, and “the state's contempt in failing to apply an extension order concerning the employment of people with disabilities in the public service.”

Malaysia

• Good Electronics reports that a roof collapsed at the Western Digital factory in Malaysia and killed an operator.

• A Malaysian news outlet reports that the Penang Department of Occupational Safety and Health (DOSH) is investigating the incident regarding a collapsed roof at an
A Malaysian news outlet reports employers will not be penalized for hiring illegal immigrant workers if they surrender them to Malaysian Immigration Department before December 31, 2014.

A Malaysian news outlet reports that labor activists and The Malaysian Employers Federation (MEF) are questioning the new policy to make foreign workers pay the full cost of medical treatment at public healthcare facilities by 2017.

A Malaysian news outlet reports MTUC suggested employers should be obligated to train low-skilled workers.

A Malaysian news outlet reports the price of RON97 gasoline will decrease by 20 cents to RM2.55 per liter from November 19, 2014.

A MTUC posted on its blog, calling for an amendment to Labor Act 1955 made in 2011, stating that it is not beneficial to workers due to the contract-based employment system.

A Malaysian news outlet reports that the MTUC (Malaysian Trade Union Congress) criticized Malaysia Airlines firing an employee for sexual harassment without a fair investigation.

A Malaysian news outlet reports the Malaysian Employers Federation (MEF) called for a new commission to be set up to handle the issue of foreign workers and a clear policy in the recruitment of foreign workers.

**North America**

- Oregon Live reported that Amazon, which operates large data centers in Morrow County, is the latest large tech company to pledge to use renewable power at its server farms.

- The San Jose Mercury News reported shuttle bus drivers who take Facebook employees to and from work will vote on 11/19/2014 on whether to unionize, hoping success at the poll will lead to others to join their campaign for better pay and working conditions.

- Sault Ste. Marie Evening News reported that Oracle has told about 60 employees that they will be laid off. This includes people in the Netherlands, Switzerland, Germany, and Spain. Managers of this unit wanted to hire more people in Romania, where the costs, particularly salaries, are far lower than they are in Western Europe. But according to one Oracle employee who is still with the company, employees across the Global Software Support unit have been talking about this move.

- International Business Times reported that Microsoft is one of Silicon Valley companies that has hired robot security guards to protect and serve the streets around north CA's technology hub. The Knightscope K5 robot security guards are fitted with lasers, GPS and heat-detecting technology, and can predict where criminals will strike next and the likelihood of future crimes.

**Vietnam**

- The future of DDoS attacks are expected to come from Vietnam, India, and Indonesia. Network World reports that these countries “might not have the most advanced Internet infrastructure, they do have a large number of insecure smartphones coming online, making them the big botnet sources for next year's distributed denial of service attacks." The article further highlights that the attackers motivation will initially be for "money" and due to the lack of controls many people may be using illegal copies of software which may contain malware.
Vietnam+ reported that Deputies at the eighth session of the 13th National Assembly passed the Law on Citizen Identification and the Law on Civil Status on November 20. The Law on Citizen Identification, which was passed with 76.66 percent of votes, is expected to lay the legal foundation for the allocation of a personal identity number to each citizen and ensure the process is implemented meticulously and in a way that helps manage society. Meanwhile, the Law on Civil Status, passed with 76.65 percent of votes, is designed to guarantee the legal frameworks on civil status, family records and citizen identity are harmonized. It will also avoid overlaps in the State management of ministries and agencies, thus preventing wastefulness and ensuring user-friendliness. This is a big step for Vietnam because Vietnam has no centralize database.

Lao Dong News reported that over 300 employees from MTV TBO Vina, a clothing manufacturing company, went on strike to protest company representatives unilaterally issued odd and strict rules for workers to follow. The company issued a rule that employees can only take 3 restroom breaks within a day. In addition the company would unilaterally change work hours without consulting with workers and failed to pay overtime when hours were unilaterally extended. The strike seems to be a wild cat strike.

Legal and Regulations

- The Alliance of Automobile Manufacturers and the Association of Global Automakers, the two leading trade associations for vehicle manufacturers, today unveiled a set of baseline protections for consumer’s personal information in the era of connected cars. The Privacy Principles for Vehicle Technologies and Services commit participating automakers to take important steps to protect the personal information retrieved from vehicles.

- On November 3, 2014, the Federal Financial Institutions Examination Council (“FFIEC”), an interagency body that prescribes principles and standards for the federal examination of financial institutions, released a set of general observations drawn from a cyber security examination work program (“Cybersecurity Assessment”) conducted at over 500 community financial institutions during the summer of 2014. The FFIEC’s report relates to both cybersecurity inherent risk and risk management practices and preparedness and includes themes and questions for management of financial institutions to consider concerning cyber security and preparedness.

- California Attorney General Kamala Harris released the state’s second Data Breach Report that confirms a rise in breaches and offers nine recommendations that will decrease the chances of security problems. To read the California Data Breach Report, click here.

On October 29, 2014, Department of Homeland Security’s Industrial Control Systems Cyber Emergency Response Team (“ICS-CERT”) published an important alert regarding a particularly destructive advanced persistent threat (“APT”) malware called BlackEnergy that can be used to damage, modify, or disrupt industrial control systems (https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01A). BlackEnergy is a malware that has been exploiting vulnerabilities in Linux- and Windows-based software since as early as January 2012.

Pharmaceuticals
Ohio lawmakers advanced a measure that would exempt disclosure of the names of manufacturers of drugs that are used in executions in the state.

The California Supreme Court agreed to review an appeal by Bristol-Myers Squibb on whether 575 people who are not state residents can join a lawsuit claiming they were harmed by its Plavix bloodthinner.

In a bid to make clinical trial results more widely available, the Obama administration has proposed new rules that require researchers in industry and academia to post findings of all studies funded by the federal government on a publicly available website. The move follows ongoing criticism that public health may be harmed because too many trial results remain hidden away.

Specialty and generic drug maker Actavis has agreed to buy Botox manufacturer Allergan for $66 billion in a move analysts say could help transform Actavis into a major pharma giant.

The FDA will require large compounding pharmacies to register each year, pay a $15,000 annual fee and report a detailed list of all the products they manufacture every six months.

Retail

A press release from Descartes Systems Group, the global leader in uniting logistics-intensive businesses in commerce, announced that the company has acquired Airclic Inc. ("Airclic"), a leading US-based provider of mobile solutions that help companies reduce the cost of delivering goods by automating traditional paper-based processes.

Internet Retailer reported that between July and September of 2014, information security company SafeNet counted 320 reported data breaches, an increase of 25% compared to the third quarter of 2013. Those security failures exposed more than 183 million customer accounts. SafeNet tracks data breaches on a quarterly basis for its Breach Level Index.

CNBC News reported that on Thursday, Walmart came under fire from the Making Change at Walmart organization, after the labor group posted an image to its Facebook page showing a food drive for employees at an Oklahoma store. Wal-Mart spokeswoman Kayla Whaling quickly responded to the criticism, saying the drive was planned by one of the store's employees, who was collecting food for two co-workers who were on a leave of absent and unable to work.

The Charlotte Observer reported that Matthews-based Family Dollar, the CEO of Dollar Tree said Thursday that he expects federal antitrust regulators will require the company to divest fewer of its stores to gain approval for the deal. The Federal Trade Commission is weighing competing offers for Family Dollar: An $8.5 billion cash-and-stock offer from Dollar Tree and a $9.1 billion all-cash hostile offer from Dollar General.

Dallas News reported that GameStop Corp. reported weaker-than-expected third-quarter results Thursday and partly blamed a delay in the release of the Assassin’s Creed Unity game. The game had been expected in October but was released early this month, pushing those sales into the fourth quarter.

The Huffington Post reported that online retailer Amazon is rolling out deals on Friday, Nov. 21, a full week ahead of the traditional Black Friday. For eight days starting on Friday, Amazon will have new sales every ten minutes, on everything from electronics to clothing to toys, the company announced on Thursday. On top of those sales, Amazon will have six special “Deals of the Day,” three on Thanksgiving day and three more on Black Friday.
There’s money to be made for any retailer who succeeds in making Instagram a shopping site. Michael Kors Holdings is taking a crack at it, hoping to nudge its 3.1 million photo-swapping followers into making purchases. The problem facing Kors and other retailers is that Instagram, a Facebook company, doesn’t make it easy to sell stuff. For all its scale and corporate participation, the photo-sharing platform is still all about photos. The outcry that Facebook set off when it bought Instagram was apparently enough to keep it from messing with that formula. Instagram doesn’t allow text and links and prices and the rest of web infrastructure that pipes users to a “buy” button.

Nearly two-thirds of Top 1000 retailers promoted a sales offer to consumers this week, and numerous e-retailers began offering deals normally reserved for the days after Thanksgiving.

More retailers are beginning to take advantage of mobile technologies that allow them to track and engage in-store shoppers.

With the help of China’s Alibaba, U.S. merchants are aiming to extend the popular online shopping day of Black Friday to Chinese consumers.

Amazon.com Inc. agreed to change some of the rules for workers at the web retailer’s warehouses in the U.S. so that employees can communicate about pay and working conditions without fear of retaliation. The deal could open the door for Amazon’s workers to unionize, because the settlement requires the online retailer to post notices at its fulfillment centers notifying employees that they have the right to form unions and work with each other for collective benefits.

Between July and September of 2014, information security company SafeNet counted 320 reported data breaches, an increase of 25% compared to the third quarter of 2013. Those security failures exposed more than 183 million customer accounts. And the retail industry was hit hard. Retailers accounted for 31% of records stolen—57,216,390 data records—in 47 data breach incidents, or 15% of the data breach incidents. The only industry accounting for more breaches and lost records was the financial industry with 77,605,972 (42%) records.

Technology

More sophisticated and more stealthy version of the NotCompatible Android Trojan continues to strengthen as an advanced mobile botnet. The malware disguises as a security patch and distributed to victims via a drive-by downloads from compromised websites and spam emails from compromised webmail accounts.

A reflected cross site scripting flaw patched overnight may affect millions of websites due to a seven-year-old flaw in a jQuery validation plugin demo script used for CAPTCHA.

CyberArk’s report which contains interviews with a variety of industry experts claims that attacks leveraging privileged accounts proceed faster and are more difficult to detect than those that rely predominately on malware or vulnerabilities. CyberArk’s data suggests that a significant part of the problem relates to inventory as organizations have “at least three or four times as many privileged accounts they have employees.”

Security companies have started detecting attacks that leverage a critical remote code execution (RCE) vulnerability in Windows, which Microsoft patched last week.

Cyber criminals have published a variety of compromised WordPress themes and plug-ins on legitimate-looking sites, tricking developers into downloading and installing them on their own sites. CryptoPHP, the malware’s name delivers compromised components, and a backdoor with a number of capabilities. It carries with it several
hardcoded domains for command-and-control communications and uses RSA encryption to protect its communications with the C2 servers.

• Cyber-criminals are attempting to capture users master password through a new variant of Citadel malware. The newest version of Citadel have been “instructed to start capturing user keystrokes when the user starts open-source password management solutions Password Safe or KeePass, or the NeXus Personal Security Client.” The Citadel Trojan is capable of bypassing most threat detection security systems and laying low until it is instructed to take action.

• A Malaysian news outlet reported that the Malaysian electronics sector could be placed on a watch list for the US Labor Department due to the Malaysian government delay in rebutting an international global labour rights group report on forced labour in Malaysia’s electronics sector.

• The U.K. government could soon require Internet service companies to keep records to identify people using a particular phone or computer and hand them over to the police upon request.

• Members of the European Parliament, backed by German officials, are preparing a draft resolution calling for the breakup of Google.

• In a sign of discontent over divisions in Silicon Valley, drivers of Facebook shuttle buses voted Wednesday night to be represented by the Teamsters union.

• AT&T Inc. said federal investigators might need a warrant to gather data about cellphone users' locations, challenging the more permissive legal framework the government has used for years. Investigators must get permission from a judge before obtaining location data from a carrier like AT&T. But the standard of proof is lower than what is required for a warrant, thanks to Supreme Court decisions in the 1970s.

---

**Telecommunications**

- FCC Chairman Tom Wheeler says that whatever final net neutrality rules the commission issues next year, will be challenged in the courts by major service providers.

- FairPoint Communications union workers’ move to hold rallies in both Boston and Montpelier, Vt., shows that they are not willing to back down in their ongoing strike over disagreement about various concessions related to company benefits.

- The FCC is asking AT&T to provide more information about comments that CEO Randall Stephenson made saying that the company would delay new fiber network investments pending the outcome of the proposed net neutrality rules.

---

**Defense**

- Researchers at Recorded Future studied Uroborous, Energetic Bear, and APT28, three main malware families out of Russia being used for cyberspying. Their research indicates China’s cyber-espionage motivations are based on economic objectives while Russia’s motivations are that they “want to show the world they are strong politically and that energy is incredibly important to them.” Uroborous -- the name used by G Data Software AG -- is also known as Epic Turla by Kaspersky Lab, Snake by BAE Systems, and SnakeNet, and has been around since at least 2008. Its main targets: governments, embassies, defense industry, research and education, and the
pharmaceutical industry. The initial attack vector is either spear phishing emails or watering hole attacks via phony Flash player updates.

- Threat actors are targeting the Tibetan nongovernmental organizations through the use of Gh0st RAT. The threat actors utilizes spear-phishing to target their attacks and exploits the CVE-2012-0158.

- The malicious Tor exit node that originated in Russia has been "tied to the APT actors wielding the MiniDuke backdoor." The malware has been dubbed "OnionDuke" by F-Secure researchers. The malware aims to collect login credentials, system and software information. Systems are infected when a user attempts to download an executable via the malicious Tor exit node.

- The European Defence Agency (EDA) and its 26 member states are considering setting up a common fund to support multi-nation research and capability projects, according to agency and EU officials.

## Law Enforcement

- High-flying drones have been spotted near airports and bridges in New York, prompting the FBI and Federal Aviation Administration to investigate. The drones were spotted by three pilots near commercial aircraft approaching John F. Kennedy International Airport. A helicopter pilot spotted two more drones near LaGuardia Airport. The drones are troublesome because they were flying at altitudes of 2,000 to 3,000 feet, far in excess of the 400-feet limit. They are seen as a distraction, and officials don't know why they are in the air, causing some unease.

- The FBI is monitoring nearly 150 Americans who traveled to Syria recently and may have joined armed groups, Reuters reports. FBI Director James Comey said he's worried that Americans may return to the U.S. with training and connections to launch a terrorist attack on the homeland.

- A man who attacked an NYPD officer last month with a hatchet was inspired by terrorists and black separatism, NBC4 New York reports. Authorities say the suspect, Zale Thompson, was politically motivated and he appears to have drawn inspiration from foreign terrorist sources like ISIL (ISIS), but there is also evidence he was focused on black separatist ideology.