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

Get Your Free Trial for the
Cyveillance Cyber Threat Center

The first cloud-based intelligence platform designed specifically for security, cyber, and threat analysts

The Cyber Threat Center is an easy-to-use platform that helps you better protect your organization with the richest and deepest collection of online threat intelligence available anywhere, and a powerful suite of tools.

What can the Cyber Threat Center do for you?

- Save You Time – Spend less time searching and filtering, and more time analyzing data, so you can be more productive
- Empower Your Team – Having all your data and tools in one place makes it easier to collaborate with other analysts
- Make You Smarter – Compare current trends to historical data to make better predictions about potential threats and targets
- Give You Actionable Insights – See threats outside your network perimeter and who's behind them so you can take proactive measures
- Keep Your Boss Informed – Customizable dashboard reports display volume, source and other managerial metrics

Put the power of Open Source threat intelligence (OSINT) to work for
Top Incidents

**Energy**
- The U.S. Department of the Treasury has given Exxon Mobil Corp. and other contractors a license to wind down operations in the Russian Arctic as the Irving-based company prepares to comply with U.S. sanctions banning joint-venture oil exploration in the area, according to a statement by Exxon. Exxon’s partnership with Russian state-owned Rosneft has been in question as the U.S. and European Union have stepped up economic sanctions in the wake of rising tensions in Ukraine. Exxon’s venture with Rosneft had been unaffected by previous rounds of sanctions, but last week the U.S. gave companies a two-week deadline to cease operations.

**Agribusiness**
- Russia, Canada and China are projected to gain farmland this century as the world warms up due to climate change, even as global crop-growing capacity may decline.

**Insurance/Healthcare**
- Federal regulators have released new guidance to educate healthcare entities and business associates about how the HIPAA Privacy Rule affects married same-sex couples. In a statement, the Department of Health and Human Services Office for Civil Rights says it developed the guidance to assist covered entities and business associates "in understanding how the 2013 decision by the Supreme Court in United States v. Windsor may affect certain of their HIPAA Privacy Rule obligations."

**Financial Services**
- Researchers stated that the credit card-stealing malware used in the attack against a leading U.S. home improvement store has been dubbed FrameworkPOS, and differs significantly from previous retailer breaches. The home improvement store attackers named their malware to resemble a piece of well-known anti-virus software, hoping investigators would see it and simply move on.

**Global Intelligence**
- A Chinese news outlet reported that due to wage arrears, hundreds of workers went on strike at the Fuji Microelectronics plant in Guangzhou. Demonstrators gathered outside the plant holding up protest banners and obstructing traffic around the facility. The strike reportedly began on Sept 15th and demonstrations took place on Sept 16th.

**Legal and Regulations**
- The Governor of New Hampshire signed a new social media law on August 1 that becomes effective September 30, 2014. Employers are barred in most instances from requiring employees or job applicants to provide log-in information for personal social media accounts. The law makes exceptions for employers who are investigating whether the social media account was involved in the unauthorized transfer of confidential, financial, or proprietary information, as well as investigations necessary to ensure compliance with laws, regulations, or workplace conduct rules.
Pharmaceuticals

- The recently revealed Dragonfly (Havex) malware is likely targeting the pharmaceutical sector, not the energy sector as previously believed. Until now, advanced cyberattacks against industry have focused on the critical energy and chemical sectors. Manufacturing management teams are advised to update their risk assessments and ensure that their cyber security defenses can withstand what are clearly highly coordinated attacks by teams of professional hackers.

Retail

- Alibaba, the Chinese e-commerce giant, secured its place in history Thursday as the largest U.S.-listed initial public offering (IPO) of all time. The stock priced at $68 per share. That’s at the top of the expected range, signaling strong demand.

Technology

- Russia is considering measures to protect its cyberspace from the “unpredictable” West, President Vladimir Putin’s spokesman said on Friday after a Russian newspaper reported said Moscow was contemplating unplugging the Internet during protests or war as early as next year.

Telecommunications

- Verizon Wireless has confirmed that it has expanded its deployment of 1700MHz/2100MHz advanced wireless services (AWS) spectrum to boost its Long Term Evolution (LTE) coverage in 22 additional markets. Verizon has dubbed its deployment of 1700MHz/2100MHz AWS spectrum for LTE as ‘XLTE’; the new network has been designed to bolster capacity on the cellco’s 700MHz LTE network. Further, the mobile giant has claimed that it now offers XLTE in more than 400 markets nationwide, equivalent to 80% of its LTE footprint.

Defense

- Hackers associated with the Chinese government successfully penetrated the computer systems of U.S. Transportation Command contractors at least 20 times in a single year, intrusions that show vulnerabilities in the military’s system to deploy troops and equipment in a crisis, a Senate Armed Services Committee investigation has found.

Law Enforcement

- Apple recently announced that it is making it impossible for the company to turn over data from most iPhones or iPads to police — even when they have a search warrant. The move, announced with the publication of a new privacy policy tied to the release of Apple’s latest mobile operating system, iOS 8, amounts to an engineering solution to a legal quandary: Rather than comply with binding court orders, Apple has reworked its latest encryption in a way that prevents the company — or anyone but the device’s owner — from gaining access to the vast troves of user data typically stored on smartphones or tablet computers.

Energy

- The U.S. Environmental Protection Agency must act to rein in methane pollution from the oil and gas industry, environmental groups said on Thursday, warning that failure to set federal standards would undermine other Obama administration efforts to address climate change. The EPA is expected to lay out a plan within months to reduce methane emissions from oil and gas drilling as a part of President Barack Obama’s broad climate action plan. A coalition of major green groups, including the Environmental Defense Fund and the Natural Resources Defense Council, urged
Obama in a letter to "swiftly" issue binding emission regulations on oil and gas production, the largest industrial source of methane.

- Article starts by discussing how the natural gas industry has often touted how fracking will bring an abundance of high paying jobs. The article points out that numerous independent studies have conclude that the industry vastly overstated the number of jobs that fracking has created, and that the economic benefits have been overblown. A growing body of research suggests that not only does the industry create fewer jobs than promised, the jobs that are created come with serious dangers for the workers who take them. Research made public late last month suggests that some of those jobs may be even more hazardous to workers than previously believed, calling into question the true benefits of the boom. The Centers for Disease Control and Prevention (CDC) has released preliminary results from its workplace hazard evaluations at unconventional oil and gas wells – and they show that workers can be exposed to high levels of benzene during fracking flowback.

- Article discusses a new study which finds that well-built fracking wells pose no threat to nearby drinking water. The study blames contamination on poor construction. So states need strong standards for well construction — to ensure, for example, that the cementing is done effectively, that there are plenty of layers of casing, that the well runs straight and has smooth sides, and so on. And states need enough trained inspectors to see that the rules are carefully followed.

- The U.S. Department of the Treasury has given Exxon Mobil Corp. and other contractors a license to wind down operations in the Russian Arctic as the Irving-based company prepares to comply with U.S. sanctions banning joint-venture oil exploration in the area, according to a statement by Exxon. Exxon's partnership with Russian state-owned Rosneft has been in question as the U.S. and European Union have stepped up economic sanctions in the wake of rising tensions in Ukraine. Exxon's venture with Rosneft had been unaffected by previous rounds of sanctions, but last week the U.S. gave companies a two-week deadline to cease operations.

- More than 20 demonstrators blocked the tracks leading to an oil train terminal near Clatskanie (OR) to protest the shipment of crude oil to the facility on the Columbia River. Protesters with the group Portland Rising Tide provided photos showing a 27-year-old activist, Sunny Glover, sitting in a tripod of 20-foot-high metal poles erected over the tracks Thursday afternoon.

- About a dozen anti-fracking protesters tried to send a message to Gov. Andrew Cuomo and local democratic party leaders at a big-bucks fundraiser on Wednesday hosted by prominent area developer Wayne LeChase. But, party leaders didn't stop to talk, and protesters couldn't get by blazer-wearing event organizers and Webster police to attend the $5,000-to-$20,000-a-ticket fundraising event because they weren't on the guest list.

- Two men were arrested after chaining themselves to pipe being laid for Vermont Gas' fracked gas pipeline. The action took place a day before the Vermont Public Service Board begins a process which could result in the revoking of the permits required for Vermont Gas to continue construction.

- Faulty wells, not deep underground fracking, is the main reason that natural gas extraction from shale rock has contaminated drinking water in parts of Texas and Pennsylvania, says a study Monday by researchers from five universities. As natural gas production increases in the United States, so, too, have reports of well water contaminated with methane. Now a study, the first to make comprehensive use of "stray gas forensics," not only found pollution in multiple wells but also identifies the culprit. "Our data clearly show that the contamination in these clusters stems from well-integrity problems such as poor casing and cementing," says co-author Thomas Darrah, assistant professor of earth science at Ohio State. While a scientist at Duke University, he led the research team, which includes experts from Duke, Stanford, Dartmouth and the University of Rochester.
RAMPS and Keepers of the Mountains are hosting the 9th annual Mountain Justice Fall Summit on Kayford Mountain, October 24th-26th. Issues to be covered include Mountaintop Removal, Fracking, Water, Health, Drug Addiction, Jails and Prisons, Colonization, Local Plants, Military Industrial Complex, Direct Action, Community Organizing, Disaster Response and much more.

Agribusiness

- President Obama directed the government to combat the rise of antibiotic-resistant bacteria, with the Agriculture Department taking a major role. The executive order signed by Obama also told FDA to eliminate agricultural use of medically important antibiotics as growth-promoting agent.
- Agricultural officials from China and the United States failed to agree at a meeting last week on how to assure U.S. shipments of distillers dried grains, an ethanol co-product used as livestock feed, does not contain unapproved genetically modified organisms.
- Three years of drought in California have withered pastures for dairy cattle and struck hard at organic herds.
- Russia, Canada and China are projected to gain farmland this century as the world warms up due to climate change, even as global crop-growing capacity may decline.
- The New Mexico Livestock Board has launched an investigation into a southern New Mexico dairy after an activist recorded video of animal abuse.

Insurance/Healthcare

- International hackers are moving up to the top of healthcare organizations’ concern lists, and those fears are beginning to be applied to reality. Just more than a month after Chinese hacker group Advanced Persistent Threat (APT) allegedly hacked into the Community Health Systems, Inc. (CHSI) network, a report announced that Russian cyber terrorists have breached American Income Life and are selling medical records.
- The Centers for Medicare and Medicaid Services will carry out 28 recommendations made by a government watchdog agency to improve the security of HealthCare.gov before the next open enrollment period for Obamacare begins Nov. 15th.
- The Office of the National Coordinator for Health Information Technology (ONC) shared news this week that Regional Extension Centers (RECs) have aided more than 100,000 healthcare organizations in EHR adoption and Stage 1 Meaningful Use attestation.
- Federal regulators have released new guidance to educate healthcare entities and business associates about how the HIPAA Privacy Rule affects married same-sex couples. In a statement, the Department of Health and Human Services Office for Civil Rights says it developed the guidance to assist covered entities and business associates “in understanding how the 2013 decision by the Supreme Court in United States v. Windsor may affect certain of their HIPAA Privacy Rule obligations.”
- Many Britons appear to take the view that honesty is not the best policy when it comes to taking out car insurance. Industry figures showed firms are uncovering almost 3,500 fraudulent applications each week.
- Michigan should create a special authority devoted to targeting auto insurance fraud and require insurers to more frequently send electronic verification of drivers’ insurance to the state, a task force recommended Wednesday.
Medical identity theft, fraud, and negligence are prevalent healthcare data breaches these days because of the integration of financial data and these incidents aren’t going away any time soon, so it’s up to organizations to figure out who the insider threats are and how to reduce those risks.

An employee at a business associate serving Aventura (Fla.) Hospital and Medical Center inappropriately accessed information on thousands of patients over a two-year period. Valesco Ventures, which provides hospital physician staffing and related services, says in a notice published in local media outlets earlier this month that an employee inappropriately accessed the patient information from Sept. 13, 2012, through June 9, 2014. Nearly 83,000 patients were impacted by the incident.

According to a recent Forrester Research brief entitled “Stolen and Lost Devices Are Putting Personal Healthcare Information at Risk,” more than 41 percent of healthcare organizations haven’t deployed endpoint encryption, despite the fact that about a third of healthcare employees work outside the office or clinic at least once a week.

William Jennings Bryan Dorn Veterans Affairs (VA) medical center has been hit with yet another lawsuit following a health data breach. On July 14, staff members first noticed that four boxes with patients’ information had gone missing. The documents were pathology records, and included veterans’ names, social security numbers and pathology reports from 1999, 2000 and 2002. However, the over 2,000 patients potentially affected were not notified until two months later.

Financial

**Financial Services**

**Activism**

- Anti-war and environmental activists held a rally in observance of International Peace Day & NYC’s ‘People’s Climate March’ in the parking lot of a leading U.S. bank branch in Springfield, MO on September 21st.

- An OWS-affiliated housing activist group will host a ‘Ghosts of Wall Street’ event in Los Angeles, CA on October 31st. The group encourages other activist organizations to plan a similar anti-Wall Street event in their home towns across the country.

- The European Environmental Foundation called on more than 160 environmental activists spanning 44 countries to unite against foundations, investors, universities, pensions, and other endowments that help fund climate change projects and demand that they drop their investments in fossil fuels. The foundation said fossil fuels need to stay in the ground if the world is to avoid some of the most catastrophic effects of climate change. The effort came as activists were gearing up for the People’s Climate March event that took place in NYC on September 21st.

- Housing activists launched a petition against a leading U.S. bank in support of a local homeowner facing eviction from her bank-owned home in Williamston, NC. The group is demanding that the bank provide her a permanent modification on her home loan. The activists stated they plan to deliver the petition to the bank in person.

- A Social Media post by a likely Anonymous hacktivist member attempted to educate his readers about the finance industry, identifying one particular leading U.S. financial services company as the core of the financial world and contributor to the 2008 economic crash. The author also provided possible insight into the financial firm’s network configuration as he commented on the firm’s massive backup server. It’s possible the hacker is attempting to rally fellow cohorts to launch a cyber-attack against the firm and U.S. financial system.
• Former homeowners who were evicted by the two GSEs for housing shared their eviction stories on September 18th at a public hearing at the Hampshire College Faculty Lounge in Amherst, MA hosted by local housing activist groups.

• Activists launched a petition targeting the Department of Housing and Urban Development's program called the Distressed Asset Stabilization Program. The petition instead proposed an alternative: Non-profit “Community Development Financial Institutions” that have a track record of successfully helping struggling homeowners and developing affordable housing. Within just 10 days, the petition gathered over 7,000 signatures.

• Housing activists in Worcester, MA held an auction protest on September 17th in support of a local homeowner facing eviction by a regional credit union.

• A national environmental activist group released a report on September 10th that warns investors of serious financial, corporate governance, and sustainability risks associated with the new gas export subsidiary of a leading U.S. power & energy company, which would own a controversial $3.8 billion liquefied natural gas export facility at Cove Point in southern Maryland. The report recommends that investors avoid buying units in the company, which is awaiting SEC approval to make an IPO on the NYSE.

• Housing activists held a “call-in” campaign on September 17th, “occupying” Attorney General Eric Holder’s phone lines in support of a former homeowner in Orange, NJ, who was evicted from her home by a leading U.S. bank.

• Activists will organize “March against Capitalism” events on November 11th in several major U.S. cities nationwide.

• UK labor activists will hold a ‘Britain Needs a Pay Raise’ march and rally in London, UK on October 18th.

• Housing activists in Lawrenceville, GA carried out a “call in” campaign on September 18th targeting the Department of Housing and Urban Development Secretary and his Chief of Staff. The activists claimed the agency never responded to the demands presented during the National Day of Action against HUD on September 9th.

• Housing activists will hold a protest march to stop all evictions and demand affordable housing in the Mission District of San Francisco, CA on October 4th.

• Numerous People’s Climate Marches occurred on September 21st in major cities throughout the U.S., with NYC selected as the primary event location. Participants rallied against “climate profiteers,” demanding more accountability and actions from corporations and the Federal Government in reducing climate change.

• An anti-Wall Street, ‘Robin Hood Tax Rally’ occurred September 21st in NYC as part of the People’s Climate March day of action. The rally called for revenue raised from HR Bill 1579 (financial transaction tax) to pay for Global Climate Change Relief.

• An activist group is promoting the September 26th release of its ‘Don’t Bank on the Bomb’ report that negatively identifies lead investors in nuclear weapons producers, which will likely include several leading U.S. financial firms.

• A National Divestment Day action organized by an international environmental organization will occur throughout Australia on October 18th in which hundreds of Australians are expected to come out to the streets to tell the leading banks that if they continue to invest in fossil fuels, they will lose the peoples’ business.

Information Security Risk

• Researchers analyzed over 150,000 phishing emails that hit the customers of a leading U.S. investment bank that recently discovered a sophisticated cyber-attack on
their systems. Dubbed the ‘Smash & Grab’ campaign, researchers found malicious emails and spoofed banking content that redirected users to a RIG exploit kit via a malicious iframe. RIG checks a machine to see if it’s vulnerable, and then installs the banking Trojan Dyre on a user’s machine.

- Researchers stated that the credit card-stealing malware used in the attack against a leading U.S. home improvement store has been dubbed FrameworkPOS, and differs significantly from previous retailer breaches. The home improvement store attackers named their malware to resemble a piece of well-known anti-virus software, hoping investigators would see it and simply move on.

- Researchers said a banking Trojan, known for its small size but powerful capabilities, has expanded the number of financial institutions from which it can collect data. Tiny Banker, also known as Tinba, was discovered around mid-2012 after it infected thousands of computers in Turkey. The malware is just 20K in size and can inject HTML fields into websites when it detects a user has navigated to a banking site, asking for a range of sensitive information banks would never request during an online session. A version analyzed by the researchers showed Tiny Banker has been customized to target numerous new financial institutions, many of which are based in the U.S.

- A controversial anti-government whistleblower organization released previously unseen copies of weaponized German surveillance malware called FinFisher. The group claims the malware is used by intelligence agencies around the world to spy on journalists, political dissidents and others, and that the new variants are making their way to market.

- Researchers said that a band of German hackers for hire raided some 300 banks, corporations and governments undetected for 12 years, possibly the longest campaign of its kind. The hackers registered 800 front businesses in the UK to target and fully compromise organizations in Germany, Switzerland, and Austria at the request of customers. The researchers said the damage done to companies since the attacks began in 2002 was “immeasurable.”

- Researchers said that e-commerce fraud jumped by nearly a quarter year-on-year to reach £110 million in the first half of 2014, while online banking fraud rose 71% to hit £29m, according to the latest stats from Financial Fraud Action UK. When it comes to online banking fraud, Financial Fraud Action UK said it believes criminals are increasingly targeting business accounts, as they often allow for higher value transactions.

- Researchers discovered an unintentional “side effect” of a popular business-oriented social networking service’s “obsession” with making sure users are “linked” with just about everyone with whom they have had contact. According to their findings, it is possible to troll the networking service and discover the email addresses of public figures including leading CEOs, celebrities and company executives.

- A new study found that more than half (54.9%) of the computers in China are infected with viruses and the number is growing for the first time in five years. China’s National Computer Virus Emergency Response Center said the country’s computer virus infection ratio grew by 9.8% year on year in 2013 after a reported decline for five consecutive years. Online banking and online payment remain top targets for computer viruses, with hackers not only stealing money, but private information as well. More than half of the government website portals investigated were susceptible to cyber-attack, as a total of 1,367 out of 2,714 government portals examined in 2013 reported security loopholes. Distorted web pages, spam emails and network theft were the biggest cyber threats last year.

- Researchers said that the Citadel Trojan, a popular program used by cybercriminals to gather banking credentials and steal money from accounts, has become the latest financial malware to be repurposed as a tool to steal industrial secrets—this time from petrochemical companies in the Middle East. The attack shows that either
cybercriminals are branching out into stealing valuable industrial secrets or that industrial and nation-state spies are using off-the-shelf malware and opportunistic infections to gather sensitive information.

**Legal, Litigation, Regulatory Risk**

- A leading U.K. bank will pay $550 million to resolve accusations of misconduct in its handling of mortgage securities sold to taxpayers before the financial crisis. The U.S. unit of the London-based lender reached the deal to end Federal Housing Finance Agency claims that the firm sold faulty mortgage bonds to the two GSEs for housing from 2005 to 2007.

- Five individuals, including three bank tellers, were arrested and charged for their alleged role in a New York-area identity theft ring that targeted customers of local banks and resulted in $850,000 in fraud losses over four years. The three bank tellers allegedly accessed and stole account numbers and Social Security numbers of hundreds of unsuspecting customers. That information was then allegedly relayed to two other defendants, who used the information to create fake documents using the stolen customers’ data, the attorney general says. The fake IDs were then used to withdraw money at bank branches in New York City, Westchester and Orange counties, as well as Long Island, Connecticut and Massachusetts, prosecutors allege.

- A Department of Justice (DoJ) proposal to amend Rule 41 of the Federal Rules of Criminal Procedure would make it easier for domestic law enforcement to hack into the computers of people attempting to protect their anonymity on the internet. The change in search and seizure rules would mean the FBI could seize targets whose location is “concealed through technological means.” Concealed through technological means is legal speak for hosted somewhere on the darknet, using Tor or proxies or making use of VPN technology.

**Operational Risk**

- A senior IT employee at a Palo Alto, California law firm specializing in business, securities, and intellectual property law was arrested for grabbing the firm’s confidential client information and using it to trade stocks. After the transactions, he sold the stock or used his options, reaping about $297,000 in profits.

- An IT staffer at a leading Nigerian bank in Isoko, Nigeria hacked into the bank’s systems and transferred $40 million to several bogus accounts before disappearing. The suspect is alleged to have conspired with a criminal gang to access the bank’s computer systems and inflate the balances of various illicit accounts.

- According to a survey of 535 banks, the consumer data breach incident that hit a Minnesota-based national retailer last year was costly for banks of all sizes and especially for community banks. More than 8% of debit cards and nearly 4% of credit cards were implicated in the breach, and banks reissued nearly every card so implicated, representing tens of millions of cards reissued in response to the single breach. The survey respondents alone reported reissuing a combined 4.1 million debit cards and 2.7 million credit cards; reissue cost averaged $9.72 per debit card and $8.11 per credit card, among these respondents.

- Members of ISIS forums are encouraging “lone wolf” bomb attacks in some of America’s most high-profile tourist locations: New York, Las Vegas and Texas. A post in an ISIS message board, created three weeks ago and resurfaced since September 15th with renewed urgency, includes a comprehensive guide to building pipe bombs using easily obtained materials like match heads, sugar and Christmas lights. The post suggests attacking Times Square and Las Vegas in particular, but also says tourist sites in Texas and metro stations throughout the U.S. would make good targets.

**Reputational Risk**

- An article published last week said that by cherry-picking which foreclosures they complete and which they ignore, banks are saddling individual borrowers with
permanent, inescapable debt while helping to create slums in already struggling communities. The vacant homes often attract drug dealers and squatters and bring down the value of surrounding properties. The article said these “zombie” homes can haunt homeowners for years and have a negative impact on neighborhoods and cities.

- An article published last week criticized a U.S. teacher’s pension management firm that is heavily invested in global tech companies whose factories are wrought with humanitarian issues.

- Continued reporting furthered a conspiracy theory that an alleged outage of a leading U.S. bank website on September 15th may have been the result of a digital jihad declared by ISIS and Al Qaeda. The author of the article warned that whether or not this is true, customers should withdraw their savings from the particular bank.

Global Intelligence

**Brazil**

- Approximately 3,500 workers went on strike at a Foxconn factory located in Jundiaí, São Paulo, Brazil, demanding changes to work and pay policies.

**China**

- A Chinese news outlet reported that due to wage arrears, hundreds of workers went on strike at the Fuji Microelectronics plant in Guangzhou. Demonstrators gathered outside the plant holding up protest banners and obstructing traffic around the facility. The strike reportedly began on Sept 15th and demonstrations took place on Sept 16th.

- On Sept 15, Baidu announced they had entered into a partnership with BMW to collaborate on driverless car technologies, with the goal of developing a semi-autonomous vehicle within the next three years.

- On 9/14/2014, a Chinese technology website reports a new malware called "MMarketPay.A" targeting Android devices spreading in China. Currently the malware infected 10 millions mobile devices and involves 9 application stores. According to the article, "MMarketPay.A" are able to make unauthorized application purchases in application stores.

- On 9/15/2014, a Chinese news outlet reports 9% of android applications in third-party application market contains malwares.

- On 9/15/2014, a Chinese news outlet reports Sina payment system contains SQL injection vulnerability.

- On 9/16/2014, a Chinese technology website contains an analysis on a malware disguise as Weixin QQ.

- On 9/16/2014, a Chinese news outlet reports the video game platform, Steam experienced a security breach and large amount of user credential has been stolen. According to the article another video game platform, Twitch has been targeted by hackers as well, by injecting malicious code to target its live chat room.

- On 9/17/2014, a Chinese news outlet reports the number of malware targeting computer increased for the first time in these 5 years. According to the article, the number of malwares increased is due to the malwares targeting large enterprises and key industries for virus spreading and attacks has increased.

- On 9/17/2014, a Chinese news outlet reports a total of 75185 websites experienced attacks in the past day. Among these attacks, there are 2,184,000 vulnerability exploitations and 360 millions DDoS attacks.
On 9/16/2014, a Chinese news outlet reports a hacker group called "The Knowns" breached Kbox (karaoke chains) membership database and have stolen 300,000 members' personal information in Singapore.

On 9/17/2014, a Chinese technology website reports FakeTaoBao-type malwares are the malwares that infect the most number of mobile devices in China.

On 9/18/2014, a Chinese news outlet reports a Japanese 16-year-old high school student arrested in Japan for DDoS attack a online game platform named Gameon.

On 9/18/2014, a Chinese anti-virus company, Dr. Web report a new ransomware called "Android.Locker.38.origin" that is able to lock user devices and demand ransom in order to unlock the devices.

On 9/18/2014, a Chinese news outlet reports 20807 among 120 millions website experienced hackers attacks on September 17, 2014. According to the article, the method of attacks used are mainly defacing.

Costica Rica

A Costa Rica media outlet reported that legislators from the ruling Citizen Action Party, Broad Front Party and Social Christian Unity Party presented a bill at the Legislative Assembly to reform the country's Labor Law to include language that would eliminate a ban on strikes in some public services sectors. That ban was approved by the previous administration of President Laura Chinchilla in October 2012. The essential public services included in the current ban are health care, public security and foreign trade. Labor Minister Víctor Morales said he would support a bill that legalizes strikes in both public and private sectors.

Germany

The German Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway, or Bundesnetzagentur ordered since April to disable 522 phone numbers suspected to distribute fraudulent short messages. Consumers responding to those unsolicited SMS received invoices for 90 EUR for "Flirt and Erotic Chats". Unpaid invoices were submitted to collection agencies. The latest 60 disabled numbers are connected to businesses in Bulgaria. The Federal Network Agency advises not to pay any related charges and consult consumer protection agencies or legal counsel if presented with an invoice.

Malaysia

On 9/11/2014, a Malaysian news outlet reports cases of dengue fever in Penang Island increased by 870 cases comparing to last year.

On 9/12/2014, MTUC posted on its blog regarding the labor dispute between Electronic Industry Employees Union Northern Region Peninsular Malaysia and Elna Sonic Sdn. Bhd.

On 9/15/2014, a Malaysian news outlet reports Malaysia and Israel are trade partners according to one of the news outlet in Israel. It is possible that this news article will stir up boycott or protest movement in Malaysia.

On 9/15/2014, a Malaysian news outlet reports confirmation from health director-general of Malaysian that there is no Ebola virus case in Malaysia.

On 9/15/2014, a Malaysian news outlet reports Singapore's Air pollution has reach unhealthy level with air pollution index recorded at 401.

On 9/17/2014, a Malaysian news outlet reports the result of a study funded by the US Department of Labor and found "force labour" is practiced in Malaysian electronics industry.

On 9/17/2014, a Malaysian news outlet reports MTUC is urging the Malaysian
government to impose a heavier penalty for employers who neglect workers' safety.

- On 9/17/2014, a Malaysian news outlet report 249 company directors has been prevented from leaving Malaysian without settling their Employees Provident Fund (EPF) contribution arrears.

**North America**

- On 9/15/2014 GigaOM reported that some IBM Global Technology Services employees have been told they and 90% of their pay as long as they retrain on hot new technologies.

- On 9/16/2014 the Progressive reported the Center for Media and Democracy/Progressive Inc. (CMD) has joined more than 50 watchdog, advocacy, and labor groups in sending a letter to Google asking it to cut its ties to the American Legislative Exchange Council (ALEC). According to the article, Google has not responded.

- On 9/18/2014 the SFGate reported that SEIU United Service Workers West will hold a protest at four Northern CA Apple store locations in San Francisco, Palo Alto, Santa Rosa, and Burlingame. The group is advocating for Apple to provide more full-time work for its security officers.

- On 9/18/2014 Reuters reported that Microsoft will close its Silicon Valley research-and-development operation as part of 2,100 layoffs.

**Vietnam**

- On 9/13/2014 FALMI, a local media source that focuses on employment news in Ho Chi Minh City, reported that the Ho Chi Minh City's People's Committee met unexpectedly on 9/11/2014 to review and provide opinions on proposed corporate incentive for Samsung Corporation's investment at Hi-Tech Park in District 9. The Committee approved of the corporate incentive to Samsung Corp. Due to Samsung's request for secrecy, the details for the incentives and Samsung's investments will be revealed at an appropriate time.

- On 9/13/2014 Tuoi Tre News reported that one out of three people in Vietnam, or 36% of the population of 90 million, now own a smartphone, nearly double last year's figure.

- On 9/18/2014 Lao Dong News reported that there was a major fire at Sakata Corporation, a squid manufacturing company. When the fire occurred over 100 workers were working at the time. Witness at the scene stated that most of the people made it outside but many people fainted after escaping and required medical assistance. According to the media source, there were 15 fire trucks at the scene of the fire.

---

**Legal and Regulations**

**New gTLDs**

- The General Availability phase for .deals will begin September 24, 2014.

- The General Availability phase for .beer, .surf will begin September 25, 2014.

- Florida’s new Florida Information Protection Act, Fl. Stat. § 501.171, became effective July 1, 2014. The new law repeals and replaces Florida’s existing data breach notification requirements (Fl. Stat. § 817.5681) with more expansive reach and enforcement in this area. The Florida Information Protection Act (FIPA) continues a trend of states enacting their own data breach and notification laws that expand beyond the scope of the federal requirements under the Health Information and Portability Act (HIPAA.).
- New York recently enacted major corporate franchise tax reform legislation generally taking effect on January 1, 2015, with some exceptions.
- FCC Form 477, Local Competition and Broadband Report, containing data as of June 30, 2014, must be filed by October 1, 2014.
- The Governor of New Hampshire signed a new social media law on August 1 that becomes effective September 30, 2014. Employers are barred in most instances from requiring employees or job applicants to provide log-in information for personal social media accounts. The law makes exceptions for employers who are investigating whether the social media account was involved in the unauthorized transfer of confidential, financial, or proprietary information, as well as investigations necessary to ensure compliance with laws, regulations, or workplace conduct rules.

---

**Pharmaceuticals**

- The recently revealed Dragonfly (Havex) malware is likely targeting the pharmaceutical sector, not the energy sector as previously believed. Until now, advanced cyberattacks against industry have focused on the critical energy and chemical sectors. Manufacturing management teams are advised to update their risk assessments and ensure that their cyber security defenses can withstand what are clearly highly coordinated attacks by teams of professional hackers.

- After months of anticipation, a Chinese court found the GlaxoSmithKline subsidiary in China guilty of bribing doctors, hospital officials and other non-government personnel, and fined the drug maker more than $490 million. This becomes the largest such penalty levied on a company in China.

- Horizon Pharma, which is based in Deerfield, Illinois, shifted its corporate address to Ireland, defying a threat by Democratic lawmakers to unwind such maneuvers retroactively. In doing so, Horizon would become the first company to complete a tax inversions that risks being overturned if legislation submitted by congressional Democrats this year becomes law.

- Novartis disclosed that another 83 employees will be laid off by year’s end from its Suffern, New York, plant, which the drug maker announced earlier this would be closed in 2016.

- The U.S. government will set up a task force and presidential advisory council to tackle the growing threat of antibiotic resistance, setting a Feb. 15 deadline for it to outline specific steps, White House advisers said on Thursday.

- The dark web gets darker with the rise of ‘Evolution’ drug market. The anonymous black market bazaar Evolution has grown dramatically, nearly tripling its sales listings in just the last five months. It now offers more than 15,000 mostly illegal products.

- .pharmacy web address to go live in early 2015. The initiative will restrict the use of .pharmacy domain names to legitimate operators that meet internet pharmacy practice standards in the countries where they operate.

- Cybercriminals abuse new TLDs in phishing and malware attacks including but are not limited to .network, .pharmacy, .enterprises, .email, etc.

---

**Retail**
Alibaba, the Chinese e-commerce giant, secured its place in history Thursday as the largest U.S.-listed initial public offering (IPO) of all time. The stock priced at $68 per share. That's at the top of the expected range, signaling strong demand.

Home Depot said Thursday that a data breach that lasted for months at its stores in the U.S. and Canada affected 56 million debit and credit cards, far more than a pre-Christmas 2013 attack on Target customers.

Online shopping's impact is taking its toll on brick-and-mortar retailers, who are now struggling to compete by offering their own spin on instant gratification and convenience. One such retailer is Sears, which last year introduced a “Shop’In” feature within its own mobile application in order to connect in-store and online shopping. Today, mobile users are offered e-coupons, price comparisons, and personalized deals, and now, online shoppers can pick up merchandise, as well as return or exchange items without having to get out of their cars.

USA Today reported that Yum Brands pulled its red star logo, apologizing profusely, just days after opening the first Banh Shop restaurant near Southern Methodist University in Dallas. An online petition pointed out that the logo was offensive to local Vietnamese residents because of its symbolic links to communism.

Milwaukee Journal Sentinel reported that Oasis Beverages, an international beer and beverage company, has agreed to acquire Pabst Brewing Co. from food industry investor C. Dean Metropoulos.

ZD Net reported Microsoft cut another 2,100 people on September 18 in round two of its previously announced planned layoff of 18,000 people. A spokesperson said the remaining cuts will be at other Microsoft locations worldwide.

MLive Michigan reported that Midwest retailer Meijer Inc. has agreed to pay a $2 million fine as part of a settlement with U.S. Consumer Product Safety Commission over the resale of 12 recalled consumer products four years ago.

USA Today reported that Apple Inc. may have unwittingly become a regulated financial institution by launching its mobile payments service, Apple Pay. Georgetown law professor Adam Levitin wrote in a blog post on Credit Slips “I think Apple is now a ‘service provider’ for purposes of the Consumer Financial Protection Act.” This would make Apple subject to examination by the newly created Consumer Financial Protection Bureau, and more broadly bound to the Unfair, Deceptive or Abusive Acts or Practices (UDAAP) monitoring of the agency.

Technology

Russia is considering measures to protect its cyberspace from the “unpredictable” West, President Vladimir Putin's spokesman said on Friday after a Russian newspaper reported said Moscow was contemplating unplugging the Internet during protests or war as early as next year.

Microsoft has let go 2,100 people, including 750 in the state of Washington, as part of its previously announced plan to cut 18,000 jobs.

Data protection regulators in Europe are working on creating a common set of guidelines for handling appeals by individuals whose requests to search engines to de-index personal information, under the region’s recent right to be forgotten ruling, have been refused.

After four long months of speculations and political maneuvering, the French Government finally announced that France is getting its first Chief Data Officer.
Chinese news outlets reported that according to reports, thirteen workers ranging in age from 19-24 have been diagnosed with leukemia; five of the cases proved fatal. While Foxconn claimed that the chemical substance in question, benzene or n-hexane, has not been used in operations for many years nor has Apple found evidence that the chemicals posed a threat, however, Apple is said to be taking this situation "very seriously" and is working very closely with Foxconn parties on the matter.

New research indicates that the amount of households in the United States using streaming media players (devices that route content from the Internet through a television) will significantly increase over the next three years. This is attributed to a record number of streaming media players added to homes last year, increasing ownership to homes with Internet access to 17% in Q2 of this year. By 2019, this percentage is projected to reach 39% of such households. These statistics do not include streaming content via Blu-ray, video game consoles, smart TVs, or other mobile devices.

Malwarebytes researchers discovered that Google’s popular DoubleClick ad network has been hijacked by malvertisers looking to infect vulnerable machines with trojan malware. Malicious ads on the site were redirecting users to sites hosting the Nuclear exploit kit. It would then check a victim’s machine to see if it was running out-of-date versions of Flash, IE or Adobe software.

Telecommunications

Verizon Wireless has confirmed that it has expanded its deployment of 1700MHz/2100MHz advanced wireless services (AWS) spectrum to boost its Long Term Evolution (LTE) coverage in 22 additional markets. Verizon has dubbed its deployment of 1700MHz/2100MHz AWS spectrum for LTE as ‘XLTE’; the new network has been designed to bolster capacity on the cellco’s 700MHz LTE network. Further, the mobile giant has claimed that it now offers XLTE in more than 400 markets nationwide, equivalent to 80% of its LTE footprint.

Defense

Hackers associated with the Chinese government successfully penetrated the computer systems of U.S. Transportation Command contractors at least 20 times in a single year, intrusions that show vulnerabilities in the military’s system to deploy troops and equipment in a crisis, a Senate Armed Services Committee investigation has found.

The deputy director of the National Security Agency said that the Intelligence Community should declassify the existence of more cyber-attacks to improve the agency’s ability to mobilize the private sector and to get help when needed.

The Mexican government has proposed an enhanced defence budget for 2015, with a projected 9% rise over spending in 2014.

As uncertainty rises over US defence spending and as the possibility of further deep defence cuts tied to sequestration raises questions over the future of the US force structure, both China and Russia are moving forward, significantly increasing their investments in defense procurement and force modernisation over the next decade.
Law Enforcement

- A man who drove up to a White House gate and refused to leave was arrested on Saturday, less than 24 hours after another man jumped the fence and made it all the way into the presidential residence before being apprehended.

- Apple recently announced that it is making it impossible for the company to turn over data from most iPhones or iPads to police — even when they have a search warrant. The move, announced with the publication of a new privacy policy tied to the release of Apple’s latest mobile operating system, iOS 8, amounts to an engineering solution to a legal quandary: Rather than comply with binding court orders, Apple has reworked its latest encryption in a way that prevents the company — or anyone but the device’s owner — from gaining access to the vast troves of user data typically stored on smartphones or tablet computers.

About Cyveillance | Solutions | Blog | Events

Cyveillance, Inc.
11091 Sunset Hills Road Suite 210
Reston, Virginia 20190

www.cyveillance.com
Contact Us
+888-243-0097

Copyright © 2014 Cyveillance, Inc.
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

Get Your Free Trial for the
Cyveillance Cyber Threat Center

The first cloud-based intelligence platform designed specifically for security, cyber, and threat analysts

The Cyber Threat Center is an easy-to-use platform that helps you better protect your organization with the richest and deepest collection of online threat intelligence available anywhere, and a powerful suite of tools.

What can the Cyber Threat Center do for you?

- Save You Time – Spend less time searching and filtering, and more time analyzing data, so you can be more productive
- Empower Your Team – Having all your data and tools in one place makes it easier to collaborate with other analysts
- Make You Smarter – Compare current trends to historical data to make better predictions about potential threats and targets
- Give You Actionable Insights – See threats outside your network perimeter and who's behind them so you can take proactive measures
- Keep Your Boss Informed – Customizable dashboard reports display volume, source and other managerial metrics

Put the power of Open Source threat intelligence (OSINT) to work for your organization today!

FREE TRIAL

Top Incidents

Energy

- The U.S. Department of the Treasury has given Exxon Mobil Corp. and other contractors a license to wind down operations in the Russian Arctic as the Irving-based company prepares to comply with U.S. sanctions banning joint-venture oil exploration in the area, according to a statement by Exxon. Exxon’s partnership with Russian
state-owned Rosneft has been in question as the U.S. and European Union have stepped up economic sanctions in the wake of rising tensions in Ukraine. Exxon’s venture with Rosneft had been unaffected by previous rounds of sanctions, but last week the U.S. gave companies a two-week deadline to cease operations.

**Agribusiness**

- Russia, Canada and China are projected to gain farmland this century as the world warms up due to climate change, even as global crop-growing capacity may decline.

**Insurance/Healthcare**

- Federal regulators have released new guidance to educate healthcare entities and business associates about how the HIPAA Privacy Rule affects married same-sex couples. In a statement, the Department of Health and Human Services Office for Civil Rights says it developed the guidance to assist covered entities and business associates "in understanding how the 2013 decision by the Supreme Court in United States v. Windsor may affect certain of their HIPAA Privacy Rule obligations."

**Financial Services**

- Researchers stated that the credit card-stealing malware used in the attack against a leading U.S. home improvement store has been dubbed FrameworkPOS, and differs significantly from previous retailer breaches. The home improvement store attackers named their malware to resemble a piece of well-known anti-virus software, hoping investigators would see it and simply move on.

**Global Intelligence**

- A Chinese news outlet reported that due to wage arrears, hundreds of workers went on strike at the Fuji Microelectronics plant in Guangzhou. Demonstrators gathered outside the plant holding up protest banners and obstructing traffic around the facility. The strike reportedly began on Sept 15th and demonstrations took place on Sept 16th.

**Legal and Regulations**

- The Governor of New Hampshire signed a new social media law on August 1 that becomes effective September 30, 2014. Employers are barred in most instances from requiring employees or job applicants to provide log-in information for personal social media accounts. The law makes exceptions for employers who are investigating whether the social media account was involved in the unauthorized transfer of confidential, financial, or proprietary information, as well as investigations necessary to ensure compliance with laws, regulations, or workplace conduct rules.

**Pharmaceuticals**

- The recently revealed Dragonfly (Havex) malware is likely targeting the pharmaceutical sector, not the energy sector as previously believed. Until now, advanced cyberattacks against industry have focused on the critical energy and chemical sectors. Manufacturing management teams are advised to update their risk assessments and ensure that their cyber security defenses can withstand what are clearly highly coordinated attacks by teams of professional hackers.

**Retail**

- Alibaba, the Chinese e-commerce giant, secured its place in history Thursday as the largest U.S.-listed initial public offering (IPO) of all time. The stock priced at $68 per share. That's at the top of the expected range, signaling strong demand.

**Technology**

- Russia is considering measures to protect its cyberspace from the “unpredictable” West, President Vladimir Putin’s spokesman said on Friday after a Russian newspaper
reported said Moscow was contemplating unplugging the Internet during protests or war as early as next year.

**Telecommunications**

- Verizon Wireless has confirmed that it has expanded its deployment of 1700MHz/2100MHz advanced wireless services (AWS) spectrum to boost its Long Term Evolution (LTE) coverage in 22 additional markets. Verizon has dubbed its deployment of 1700MHz/2100MHz AWS spectrum for LTE as ‘XLTE’; the new network has been designed to bolster capacity on the cellco’s 700MHz LTE network. Further, the mobile giant has claimed that it now offers XLTE in more than 400 markets nationwide, equivalent to 80% of its LTE footprint.

**Defense**

- Hackers associated with the Chinese government successfully penetrated the computer systems of U.S. Transportation Command contractors at least 20 times in a single year, intrusions that show vulnerabilities in the military’s system to deploy troops and equipment in a crisis, a Senate Armed Services Committee investigation has found.

**Law Enforcement**

- Apple recently announced that it is making it impossible for the company to turn over data from most iPhones or iPads to police — even when they have a search warrant. The move, announced with the publication of a new privacy policy tied to the release of Apple’s latest mobile operating system, iOS 8, amounts to an engineering solution to a legal quandary: Rather than comply with binding court orders, Apple has reworked its latest encryption in a way that prevents the company — or anyone but the device’s owner — from gaining access to the vast troves of user data typically stored on smartphones or tablet computers.

**Energy**

- The U.S. Environmental Protection Agency must act to rein in methane pollution from the oil and gas industry, environmental groups said on Thursday, warning that failure to set federal standards would undermine other Obama administration efforts to address climate change. The EPA is expected to lay out a plan within months to reduce methane emissions from oil and gas drilling as a part of President Barack Obama’s broad climate action plan. A coalition of major green groups, including the Environmental Defense Fund and the Natural Resources Defense Council, urged Obama in a letter to “swiftly” issue binding emission regulations on oil and gas production, the largest industrial source of methane.

- Article starts by discussing how the natural gas industry has often touted how fracking will bring an abundance of high paying jobs. The article points out that numerous independent studies have conclude that the industry vastly overstated the number of jobs that fracking has created, and that the economic benefits have been overblown. A growing body of research suggests that not only does the industry create fewer jobs than promised, the jobs that are created come with serious dangers for the workers who take them. Research made public late last month suggests that some of those jobs may be even more hazardous to workers than previously believed, calling into question the true benefits of the boom. The Centers for Disease Control and Prevention (CDC) has released preliminary results from its workplace hazard evaluations at unconventional oil and gas wells – and they show that workers can be exposed to high levels of benzene during fracking flowback.

- Article discusses a new study which finds that well-built fracking wells pose no threat to nearby drinking water. The study blames contamination on poor construction. So
states need strong standards for well construction — to ensure, for example, that the cementing is done effectively, that there are plenty of layers of casing, that the well runs straight and has smooth sides, and so on. And states need enough trained inspectors to see that the rules are carefully followed.

- The U.S. Department of the Treasury has given Exxon Mobil Corp. and other contractors a license to wind down operations in the Russian Arctic as the Irving-based company prepares to comply with U.S. sanctions banning joint-venture oil exploration in the area, according to a statement by Exxon. Exxon’s partnership with Russian state-owned Rosneft has been in question as the U.S. and European Union have stepped up economic sanctions in the wake of rising tensions in Ukraine. Exxon’s venture with Rosneft had been unaffected by previous rounds of sanctions, but last week the U.S. gave companies a two-week deadline to cease operations.

- More than 20 demonstrators blocked the tracks leading to an oil train terminal near Clatskanie (OR) to protest the shipment of crude oil to the facility on the Columbia River. Protesters with the group Portland Rising Tide provided photos showing a 27-year-old activist, Sunny Glover, sitting in a tripod of 20-foot-high metal poles erected over the tracks Thursday afternoon.

- About a dozen anti-fracking protesters tried to send a message to Gov. Andrew Cuomo and local democratic party leaders at a big-bucks fundraiser on Wednesday hosted by prominent area developer Wayne LeChase. But, party leaders didn’t stop to talk, and protesters couldn’t get by blazer-wearing event organizers and Webster police to attend the $5,000-to-$20,000-a-ticket fundraising event because they weren’t on the guest list.

- Two men were arrested after chaining themselves to pipe being laid for Vermont Gas’ fracked gas pipeline. The action took place a day before the Vermont Public Service Board begins a process which could result in the revoking of the permits required for Vermont Gas to continue construction.

- Faulty wells, not deep underground fracking, is the main reason that natural gas extraction from shale rock has contaminated drinking water in parts of Texas and Pennsylvania, says a study Monday by researchers from five universities. As natural gas production increases in the United States, so, too, have reports of well water contaminated with methane. Now a study, the first to make comprehensive use of “stray gas forensics,” not only found pollution in multiple wells but also identifies the culprit. "Our data clearly show that the contamination in these clusters stems from well-integrity problems such as poor casing and cementing," says co-author Thomas Darrah, assistant professor of earth science at Ohio State. While a scientist at Duke University, he led the research team, which includes experts from Duke, Stanford, Dartmouth and the University of Rochester.

- RAMPS and Keepers of the Mountains are hosting the 9th annual Mountain Justice Fall Summit on Kayford Mountain, October 24th-26th. Issues to be covered include Mountaintop Removal, Fracking, Water, Health, Drug Addiction, Jails and Prisons, Colonization, Local Plants, Military Industrial Complex, Direct Action, Community Organizing, Disaster Response and much more.

---

**Agribusiness**

- President Obama directed the government to combat the rise of antibiotic-resistant bacteria, with the Agriculture Department taking a major role. The executive order signed by Obama also told FDA to eliminate agricultural use of medically important antibiotics as growth-promoting agent.

- Agricultural officials from China and the United States failed to agree at a meeting last week on how to assure U.S. shipments of distillers dried grains, an ethanol co-product.
used as livestock feed, does not contain unapproved genetically modified organisms.

- Three years of drought in California have withered pastures for dairy cattle and struck hard at organic herds.

- Russia, Canada and China are projected to gain farmland this century as the world warms up due to climate change, even as global crop-growing capacity may decline.

- The New Mexico Livestock Board has launched an investigation into a southern New Mexico dairy after an activist recorded video of animal abuse.

## Insurance/Healthcare

- International hackers are moving up to the top of healthcare organizations’ concern lists, and those fears are beginning to be applied to reality. Just more than a month after Chinese hacker group Advanced Persistent Threat (APT) allegedly hacked into the Community Health Systems, Inc. (CHSI) network, a report announced that Russian cyber terrorists have breached American Income Life and are selling medical records.

- The Centers for Medicare and Medicaid Services will carry out 28 recommendations made by a government watchdog agency to improve the security of HealthCare.gov before the next open enrollment period for Obamacare begins Nov. 15th.

- The Office of the National Coordinator for Health Information Technology (ONC) shared news this week that Regional Extension Centers (RECs) have aided more than 100,000 healthcare organizations in EHR adoption and Stage 1 Meaningful Use attestation.

- Federal regulators have released new guidance to educate healthcare entities and business associates about how the HIPAA Privacy Rule affects married same-sex couples. In a statement, the Department of Health and Human Services Office for Civil Rights says it developed the guidance to assist covered entities and business associates “in understanding how the 2013 decision by the Supreme Court in United States v. Windsor may affect certain of their HIPAA Privacy Rule obligations.”

- Many Britons appear to take the view that honesty is not the best policy when it comes to taking out car insurance. Industry figures showed firms are uncovering almost 3,500 fraudulent applications each week.

- Michigan should create a special authority devoted to targeting auto insurance fraud and require insurers to more frequently send electronic verification of drivers’ insurance to the state, a task force recommended Wednesday.

- Medical identity theft, fraud, and negligence are prevalent healthcare data breaches these days because of the integration of financial data and these incidents aren’t going away any time soon, so it’s up to organizations to figure out who the insider threats are and how to reduce those risks.

- An employee at a business associate serving Aventura (Fla.) Hospital and Medical Center inappropriately accessed information on thousands of patients over a two-year period. Valesco Ventures, which provides hospital physician staffing and related services, says in a notice published in local media outlets earlier this month that an employee inappropriately accessed the patient information from Sept. 13, 2012, through June 9, 2014. Nearly 83,000 patients were impacted by the incident.

- According to a recent Forrester Research brief entitled “Stolen and Lost Devices Are Putting Personal Healthcare Information at Risk,” more than 41 percent of healthcare organizations haven’t deployed endpoint encryption, despite the fact that about a third of healthcare employees work outside the office or clinic at least once a week.
William Jennings Bryan Dorn Veterans Affairs (VA) medical center has been hit with yet another lawsuit following a health data breach. On July 14, staff members first noticed that four boxes with patients’ information had gone missing. The documents were pathology records, and included veterans’ names, social security numbers and pathology reports from 1999, 2000 and 2002. However, the over 2,000 patients potentially affected were not notified until two months later.

Financial

Financial Services

Activism

- Anti-war and environmental activists held a rally in observance of International Peace Day & NYC’s ‘People’s Climate March’ in the parking lot of a leading U.S. bank branch in Springfield, MO on September 21st.

- An OWS-affiliated housing activist group will host a ‘Ghosts of Wall Street’ event in Los Angeles, CA on October 31st. The group encourages other activist organizations to plan a similar anti-Wall Street event in their home towns across the country.

- The European Environmental Foundation called on more than 160 environmental activists spanning 44 countries to unite against foundations, investors, universities, pensions, and other endowments that help fund climate change projects and demand that they drop their investments in fossil fuels. The foundation said fossil fuels need to stay in the ground if the world is to avoid some of the most catastrophic effects of climate change. The effort came as activists were gearing up for the People’s Climate March event that took place in NYC on September 21st.

- Housing activists launched a petition against a leading U.S. bank in support of a local homeowner facing eviction from her bank-owned home in Williamston, NC. The group is demanding that the bank provide her a permanent modification on her home loan. The activists stated they plan to deliver the petition to the bank in person.

- A Social Media post by a likely Anonymous hacktivist member attempted to educate his readers about the finance industry, identifying one particular leading U.S. financial services company as the core of the financial world and contributor to the 2008 economic crash. The author also provided possible insight into the financial firm’s network configuration as he commented on the firm’s massive backup server. It’s possible the hacker is attempting to rally fellow cohorts to launch a cyber-attack against the firm and U.S. financial system.

- Former homeowners who were evicted by the two GSEs for housing shared their eviction stories on September 18th at a public hearing at the Hampshire College Faculty Lounge in Amherst, MA hosted by local housing activist groups.

- Activists launched a petition targeting the Department of Housing and Urban Development's program called the Distressed Asset Stabilization Program. The petition instead proposed an alternative: Non-profit “Community Development Financial Institutions” that have a track record of successfully helping struggling homeowners and developing affordable housing. Within just 10 days, the petition gathered over 7,000 signatures.

- Housing activists in Worcester, MA held an auction protest on September 17th in support of a local homeowner facing eviction by a regional credit union.

- A national environmental activist group released a report on September 10th that warns investors of serious financial, corporate governance, and sustainability risks associated with the new gas export subsidiary of a leading U.S. power & energy
company, which would own a controversial $3.8 billion liquefied natural gas export facility at Cove Point in southern Maryland. The report recommends that investors avoid buying units in the company, which is awaiting SEC approval to make an IPO on the NYSE.

- Housing activists held a “call-in” campaign on September 17th, “occupying” Attorney General Eric Holder’s phone lines in support of a former homeowner in Orange, NJ, who was evicted from her home by a leading U.S. bank.

- Activists will organize “March against Capitalism” events on November 11th in several major U.S. cities nationwide.

- UK labor activists will hold a ‘Britain Needs a Pay Raise’ march and rally in London, UK on October 18th.

- Housing activists in Lawrenceville, GA carried out a “call in” campaign on September 18th targeting the Department of Housing and Urban Development Secretary and his Chief of Staff. The activists claimed the agency never responded to the demands presented during the National Day of Action against HUD on September 9th.

- Housing activists will hold a protest march to stop all evictions and demand affordable housing in the Mission District of San Francisco, CA on October 4th.

- Numerous People’s Climate Marches occurred on September 21st in major cities throughout the U.S., with NYC selected as the primary event location. Participants rallied against “climate profiteers,” demanding more accountability and actions from corporations and the Federal Government in reducing climate change.

- An anti-Wall Street, ‘Robin Hood Tax Rally’ occurred September 21st in NYC as part of the People’s Climate March day of action. The rally called for revenue raised from HR Bill 1579 (financial transaction tax) to pay for Global Climate Change Relief.

- An activist group is promoting the September 26th release of its ‘Don’t Bank on the Bomb’ report that negatively identifies lead investors in nuclear weapons producers, which will likely include several leading U.S. financial firms.

- A National Divestment Day action organized by an international environmental organization will occur throughout Australia on October 18th in which hundreds of Australians are expected to come out to the streets to tell the leading banks that if they continue to invest in fossil fuels, they will lose the peoples’ business.

**Information Security Risk**

- Researchers analyzed over 150,000 phishing emails that hit the customers of a leading U.S. investment bank that recently discovered a sophisticated cyber-attack on their systems. Dubbed the ‘Smash & Grab’ campaign, researchers found malicious emails and spoofed banking content that redirected users to a RIG exploit kit via a malicious iframe. RIG checks a machine to see if it’s vulnerable, and then installs the banking Trojan Dyre on a user’s machine.

- Researchers stated that the credit card-stealing malware used in the attack against a leading U.S. home improvement store has been dubbed FrameworkPOS, and differs significantly from previous retailer breaches. The home improvement store attackers named their malware to resemble a piece of well-known anti-virus software, hoping investigators would see it and simply move on.

- Researchers said a banking Trojan, known for its small size but powerful capabilities, has expanded the number of financial institutions from which it can collect data. Tiny Banker, also known as Tinba, was discovered around mid-2012 after it infected thousands of computers in Turkey. The malware is just 20K in size and can inject HTML fields into websites when it detects a user has navigated to a banking site, asking for a range of sensitive information banks would never request during an online
session. A version analyzed by the researchers showed Tiny Banker has been customized to target numerous new financial institutions, many of which are based in the U.S.

- A controversial anti-government whistleblower organization released previously unseen copies of weaponized German surveillance malware called FinFisher. The group claims the malware is used by intelligence agencies around the world to spy on journalists, political dissidents and others, and that the new variants are making their way to market.

- Researchers said that a band of German hackers for hire raided some 300 banks, corporations and governments undetected for 12 years, possibly the longest campaign of its kind. The hackers registered 800 front businesses in the UK to target and fully compromise organizations in Germany, Switzerland, and Austria at the request of customers. The researchers said the damage done to companies since the attacks began in 2002 was "immeasurable."

- Researchers said that e-commerce fraud jumped by nearly a quarter year-on-year to reach £110 million in the first half of 2014, while online banking fraud rose 71% to hit £29m, according to the latest stats from Financial Fraud Action UK. When it comes to online banking fraud, Financial Fraud Action UK said it believes criminals are increasingly targeting business accounts, as they often allow for higher value transactions.

- Researchers discovered an unintentional "side effect" of a popular business-oriented social networking service’s "obsession" with making sure users are "linked" with just about everyone with whom they have had contact. According to their findings, it is possible to troll the networking service and discover the email addresses of public figures including leading CEOs, celebrities and company executives.

- A new study found that more than half (54.9%) of the computers in China are infected with viruses and the number is growing for the first time in five years. China’s National Computer Virus Emergency Response Center said the country’s computer virus infection ratio grew by 9.8% year on year in 2013 after a reported decline for five consecutive years. Online banking and online payment remain top targets for computer viruses, with hackers not only stealing money, but private information as well. More than half of the government website portals investigated were susceptible to cyber-attack, as a total of 1,367 out of 2,714 government portals examined in 2013 reported security loopholes. Distorted web pages, spam emails and network theft were the biggest cyber threats last year.

- Researchers said that the Citadel Trojan, a popular program used by cybercriminals to gather banking credentials and steal money from accounts, has become the latest financial malware to be repurposed as a tool to steal industrial secrets—this time from petrochemical companies in the Middle East. The attack shows that either cybercriminals are branching out into stealing valuable industrial secrets or that industrial and nation-state spies are using off-the-shelf malware and opportunistic infections to gather sensitive information.

### Legal, Litigation, Regulatory Risk

- A leading U.K. bank will pay $550 million to resolve accusations of misconduct in its handling of mortgage securities sold to taxpayers before the financial crisis. The U.S. unit of the London-based lender reached the deal to end Federal Housing Finance Agency claims that the firm sold faulty mortgage bonds to the two GSEs for housing from 2005 to 2007.

- Five individuals, including three bank tellers, were arrested and charged for their alleged role in a New York-area identity theft ring that targeted customers of local banks and resulted in $850,000 in fraud losses over four years. The three bank tellers allegedly accessed and stole account numbers and Social Security numbers of hundreds of unsuspecting customers. That information was then allegedly relayed to two other defendants, who used the information to create fake documents using the
stolen customers’ data, the attorney general says. The fake IDs were then used to withdraw money at bank branches in New York City, Westchester and Orange counties, as well as Long Island, Connecticut and Massachusetts, prosecutors allege.

- A Department of Justice (DoJ) proposal to amend Rule 41 of the Federal Rules of Criminal Procedure would make it easier for domestic law enforcement to hack into the computers of people attempting to protect their anonymity on the internet. The change in search and seizure rules would mean the FBI could seize targets whose location is “concealed through technological means.” Concealed through technological means is legal speak for hosted somewhere on the darknet, using Tor or proxies or making use of VPN technology.

**Operational Risk**

- A senior IT employee at a Palo Alto, California law firm specializing in business, securities, and intellectual property law was arrested for grabbing the firm’s confidential client information and using it to trade stocks. After the transactions, he sold the stock or used his options, reaping about $297,000 in profits.

- An IT staffer at a leading Nigerian bank in Isoko, Nigeria hacked into the bank’s systems and transferred $40 million to several bogus accounts before disappearing. The suspect is alleged to have conspired with a criminal gang to access the bank’s computer systems and inflate the balances of various illicit accounts.

- According to a survey of 535 banks, the consumer data breach incident that hit a Minnesota-based national retailer last year was costly for banks of all sizes and especially for community banks. More than 8% of debit cards and nearly 4% of credit cards were implicated in the breach, and banks reissued nearly every card so implicated, representing tens of millions of cards reissued in response to the single breach. The survey respondents alone reported reissuing a combined 4.1 million debit cards and 2.7 million credit cards; reissue cost averaged $9.72 per debit card and $8.11 per credit card, among these respondents.

- Members of ISIS forums are encouraging “lone wolf” bomb attacks in some of America’s most high-profile tourist locations: New York, Las Vegas and Texas. A post in an ISIS message board, created three weeks ago and resurfaced since September 15th with renewed urgency, includes a comprehensive guide to building pipe bombs using easily obtained materials like match heads, sugar and Christmas lights. The post suggests attacking Times Square and Las Vegas in particular, but also says tourist sites in Texas and metro stations throughout the U.S. would make good targets.

**Reputational Risk**

- An article published last week said that by cherry-picking which foreclosures they complete and which they ignore, banks are saddling individual borrowers with permanent, inescapable debt while helping to create slums in already struggling communities. The vacant homes often attract drug dealers and squatters and bring down the value of surrounding properties. The article said these “zombie” homes can haunt homeowners for years and have a negative impact on neighborhoods and cities.

- An article published last week criticized a U.S. teacher’s pension management firm that is heavily invested in global tech companies whose factories are wrought with humanitarian issues.

- Continued reporting furthered a conspiracy theory that an alleged outage of a leading U.S. bank website on September 15th may have been the result of a digital jihad declared by ISIS and Al Qaeda. The author of the article warned that whether or not this is true, customers should withdraw their savings from the particular bank.
Global Intelligence

Brazil

- Approximately 3,500 workers went on strike at a Foxconn factory located in Jundiaí, São Paulo, Brazil, demanding changes to work and pay policies.

China

- A Chinese news outlet reported that due to wage arrears, hundreds of workers went on strike at the Fuji Microelectronics plant in Guangzhou. Demonstrators gathered outside the plant holding up protest banners and obstructing traffic around the facility. The strike reportedly began on Sept 15th and demonstrations took place on Sept 16th.

- On Sept 15, Baidu announced they had entered into a partnership with BMW to collaborate on driverless car technologies, with the goal of developing a semi-autonomous vehicle within the next three years.

- On 9/14/2014, a Chinese technology website reports a new malware called "MMarketPay.A" targeting Android devices spreading in China. Currently the malware infected 10 millions mobile devices and involves 9 application stores. According to the article, "MMarketPay.A" are able to make unauthorized application purchases in application stores.

- On 9/15/2014, a Chinese news outlet reports 9% of android applications in third-party application market contains malwares.

- On 9/15/2014, a Chinese news outlet reports Sina payment system contains SQL injection vulnerability.

- On 9/16/2014, a Chinese news outlet reports 9% of android applications in third-party application market contains malwares.

- On 9/16/2014, a Chinese technology website contains an analysis on a malware disguised as Weixin QQ.

- On 9/16/2014, a Chinese news outlet reports the video game platform, Steam experienced a security breach and large amount of user credential has been stolen. According to the article another video game platform, Twitch has been targeted by hackers as well, by injecting malicious code to target its live chat room.

- On 9/17/2014, a Chinese news outlet reports the number of malware targeting computer increased for the first time in these 5 years. According to the article, the number of malwares increased is due to the malwares targeting large enterprises and key industries for virus spreading and attacks has increased.

- On 9/17/2014, a Chinese news outlet reports a total of 75185 websites experienced attacks in the past day. Among these attacks, there are 2,184,000 vulnerability exploitations and 360 millions DDoS attacks.

- On 9/16/2014, a Chinese news outlet reports a hacker group called "The Knowns" breached Kbox (karaoke chains) membership database and have stolen 300,000 members' personal information in Singapore.

- On 9/17/2014, a Chinese technology website reports FakeTaoBao-type malwares are the malwares that infect the most number of mobile devices in China.

- On 9/18/2014, a Chinese news outlet reports a Japanese 16-year-old high school student arrested in Japan for DDoS attack a online game platform named Gameon.

- On 9/18/2014, a Chinese anti-virus company, Dr. Web report a new ransomware called "AndroidLocker.38.origin" that is able to lock user devices and demand ransom in order to unlock the devices.

- On 9/18/2014, a Chinese news outlet reports 20807 among 120 millions website
experienced hackers attacks on September 17, 2014. According to the article, the method of attacks used are mainly defacing.

Costica Rica

- A Costa Rica media outlet reported that legislators from the ruling Citizen Action Party, Broad Front Party and Social Christian Unity Party presented a bill at the Legislative Assembly to reform the country’s Labor Law to include language that would eliminate a ban on strikes in some public services sectors. That ban was approved by the previous administration of President Laura Chinchilla in October 2012. The essential public services included in the current ban are health care, public security and foreign trade. Labor Minister Víctor Morales said he would support a bill that legalizes strikes in both public and private sectors.

Germany

- The German Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway, or Bundesnetzagentur ordered since April to disable 522 phone numbers suspected to distribute fraudulent short messages. Consumers responding to those unsolicited SMS received invoices for 90 EUR for “Flirt and Erotic Chats”. Unpaid invoices were submitted to collection agencies. The latest 60 disabled numbers are connected to businesses in Bulgaria. The Federal Network Agency advises not to pay any related charges and consult consumer protection agencies or legal counsel if presented with an invoice.

Malaysia

- On 9/11/2014, a Malaysian news outlet reports cases of dengue fever in Penang Island increased by 870 cases comparing to last year.

- On 9/12/2014, MTUC posted on its blog regarding the labor dispute between Electronic Industry Employees Union Northern Region Peninsular Malaysia and Elna Sonic Sdn. Bhd.

- On 9/15/2014, a Malaysian news outlet reports Malaysia and Israel are trade partners according to one of the news outlet in Israel. It is possible that this news article will stir up boycott or protest movement in Malaysia.

- On 9/15/2014, a Malaysian news outlet reports confirmation from health director-general of Malaysian that there is no Ebola virus case in Malaysia.

- On 9/15/2014, a Malaysian news outlet reports Singapore’s Air pollution has reach unhealthy level with air pollution index recorded at 401.

- On 9/17/2014, a Malaysian news outlet reports the result of a study funded by the US Department of Labor and found “force labour” is practiced in Malaysian electronics industry.

- On 9/17/2014, a Malaysian news outlet reports MTUC is urging the Malaysian government to impose a heavier penalty for employers who neglect workers’ safety.

- On 9/17/2014, a Malaysian news outlet report 249 company directors has been prevented from leaving Malaysian without settling their Employees Provident Fund (EPF) contribution arrears.

North America

- On 9/15/2014 GigaOM reported that some IBM Global Technology Services employees have been told they and 90% of their pay as long as they retrain on hot new technologies.

- On 9/16/2014 the Progressive reported the Center for Media and Democracy/Progressive Inc. (CMD) has joined more than 50 watchdog, advocacy, and labor groups in sending a letter to Google asking it to cut its ties to the American
Legislative Exchange Council (ALEC). According to the article, Google has not responded.

- On 9/18/2014 the SFGate reported that SEIU United Service Workers West will hold a protest at four Northern CA Apple store locations in San Francisco, Palo Alto, Santa Rosa, and Burlingame. The group is advocating for Apple to provide more full-time work for its security officers.

- On 9/18/2014 Reuters reported that Microsoft will close its Silicon Valley research-and-development operation as part of 2,100 layoffs.

**Vietnam**

- On 9/13/2014 FALMI, a local media source that focuses on employment news in Ho Chi Minh City, reported that the Ho Chi Minh City's People's Committee met unexpectedly on 9/11/2014 to review and provide opinions on proposed corporate incentive for Samsung Corporation's investment at Hi-Tech Park in District 9. The Committee approved of the corporate incentive to Samsung Corp. Due to Samsung's request for secrecy, the details for the incentives and Samsung's investments will be revealed at an appropriate time.

- On 9/13/2014 Tuoi Tre News reported that one out of three people in Vietnam, or 36% of the population of 90 million, now own a smartphone, nearly double last year's figure.

- On 9/18/2014 Lao Dong News reported that there was a major fire at Sakata Corporation, a squid manufacturing company. When the fire occurred over 100 workers were working at the time. Witness at the scene stated that most of the people made it outside but many people fainted after escaping and required medical assistance. According to the media source, there were 15 fire trucks at the scene of the fire.

---

**Legal and Regulations**

**New gTLDs**

- The General Availability phase for .deals will begin September 24, 2014.
- The General Availability phase for .beer, .surf will begin September 25, 2014.

- Florida’s new Florida Information Protection Act, Fl. Stat. § 501.171, became effective July 1, 2014. The new law repeals and replaces Florida’s existing data breach notification requirements (Fl. Stat. § 817.5681) with more expansive reach and enforcement in this area. The Florida Information Protection Act (FIPA) continues a trend of states enacting their own data breach and notification laws that expand beyond the scope of the federal requirements under the Health Information and Portability Act (HIPAA.).

- New York recently enacted major corporate franchise tax reform legislation generally taking effect on January 1, 2015, with some exceptions.

- FCC Form 477, Local Competition and Broadband Report, containing data as of June 30, 2014, must be filed by October 1, 2014.

- The Governor of New Hampshire signed a new social media law on August 1 that becomes effective September 30, 2014. Employers are barred in most instances from requiring employees or job applicants to provide log-in information for personal social media accounts. The law makes exceptions for employers who are investigating whether the social media account was involved in the unauthorized transfer of confidential, financial, or proprietary information, as well as investigations necessary to ensure compliance with laws, regulations, or workplace conduct rules.