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
- Pharmaceuticals
- Retail
- Technology
- Telecommunications
- Defense
- Law Enforcement

Turning Data into Threat Intelligence: A Case Study

Eric Olson
Vice President
Product Strategy

James Carnall
Vice President
Cyber Intelligence Division

October 23, 2014

Save Your Spot - October 23 Webinar

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

Register Now
Top Incidents

**Energy**
- Pastebin user ‘HotelMoscow’ promoting a hacking campaign dubbed ‘#OpRemember’ to launch on November 5th that is set to target "the global banking cartels, the oil and gas industry, the corrupt governments of the world, the bio-tech industry, and the mega-corporations that control our planet."

**Agribusiness**
- Start-up companies such as FarmLogs and 640 Labs are in the hunt for customers along with agribusiness giants Deere, Pioneer and Monsanto in the new agricultural field of Big Data.

**Insurance/Healthcare**
- Federal authorities are ramping up efforts to crack down on healthcare fraud, announcing plans to prosecute top executives at hospitals and other organizations involved with fraud - and target other fraudsters as well.

**Financial Services**
- A new study said Russian-speaking cybercrime groups are targeting primarily US-based systems and online banking accounts. Qbot (aka Qakbot) botnet of 500,000 infected systems sniffed ‘conversations,’ including account credentials, for 800,000 online banking transactions, with 59% of sniffed sessions representing accounts at five of the largest U.S. banks.

**Global Intelligence**
- On 10/7/2014 Forbes reported that the Supreme Court heard the case and decide on the question if Amazon workers should be paid for security screening. The decision will have serious ramifications for 76 million hourly workers. After clocking out at the end of a shift, Amazon workers had to pass through security checks before leaving the building to ensure they didn’t steal anything from Amazon. The security screenings often involved waiting in long lines, sometimes taking half an hour to clear. Workers were not paid for the time they spent during security checks.

**Pharmaceuticals**
- Drugmaker GlaxoSmithKline, which was slapped with a record $489 million fine for corruption in China last month, said on Tuesday it was looking into allegations of corruption in the United Arab Emirates. Britain’s biggest pharmaceuticals group confirmed the investigation following allegations of improper payments set out in a whistleblower’s email sent to its top management on Monday.

**Retail**
- Daily Finance reported that ice cream and fast-food restaurant chain Dairy Queen has confirmed a security breach that may have compromised the payment card information of customers at several hundred locations across 46 US states. Computers at Dairy Queen locations were infected by Backoff malware.

**Technology**
- Variant of the Rovnix malware has additional features including a new domain generation algorithm and secure transmission channel for communicating with command-and-control servers.

**Telecommunications**
Internet service providers in Denmark have reached an agreement with a leading anti-piracy group. Rights Alliance will only need to obtain a single pirate site blocking order against one ISP and all the rest will voluntarily block the same domains. While the entertainment industries are capable of obtaining blocking injunctions against pirate sites, each action has to be targeted at a specific service provider. That means rival ISPs are free to carry on providing access while an injunction might be issued against one ISP.

**Defense**

Taiwan’s premier warns of increasing cyber-attacks from China are growing. The warning comes after the FBI warned that China is waging cyber-war against the United States.

**Law Enforcement**

The Justice Department is mulling whether to investigate NYPD’s use of the controversial crime fighting strategy known as “broken windows.” The Justice Department Civil Rights Division is considering a request from six members of Congress to investigate whether black people and Hispanics are disproportionately affected by quality-of-life violations.

---

**Energy**

- A large majority of Canadians would support a moratorium on fracking until there is conclusive evidence that it’s safe, according to a new poll. Seventy per cent of respondents said they would back “a national moratorium on fracking until it is scientifically proven to be safe,” according to the survey carried out by EKOS for the Council of Canadians, a group that has been critical of fracking operations. Even in Alberta, where the public tends to overwhelmingly support the oil industry, 62 per cent of respondents said they would back a moratorium.

- The Guardian reports that Lego will not renew its marketing contract with Shell after coming under sustained pressure from Greenpeace to end a partnership that dates to the 1960s.

- Activists with Frack Free North Carolina are expected to deliver a 50,000-signature petition to Governor McCrory on Tuesday, Oct. 14. The petition asks the Governor to reinstate NC’s ban on fracking.

- The Great March for Climate Action, from Los Angeles to Washington, DC, will be in Pittsburgh, PA on Tuesday, Oct. 14. Public appearances will urge the City of Pittsburgh to divest its portfolio from fossil fuels. University of Pittsburgh students will also speak on their divestment campaign. The March is passing through Pennsylvania, and is expected to cross into Maryland on Oct. 25.

- The Earth at Risk 2014 Conference will be held in San Francisco, Nov. 22-23.

- Organizing for Action (OFA) is getting behind tech companies' dismissal of the American Legislative Exchange Council (ALEC) over its stance on climate change. The OFA, the offshoot of President Obama's 2012 campaign, commended Google on Wednesday for severing ties with the group in an email pitch, which asked supporters sign their name to a petition calling for the Environmental Protection Agency to adopt Obama's clean power plan.

- Pastebin user 'HotelMoscow' promoting a hacking campaign dubbed '#OpRemember' to launch on November 5th that is set to target "the global banking cartels, the oil and gas industry, the corrupt governments of the world, the bio-tech industry, and the mega-corporations that control our planet."
Greenpeace volunteers delivered a message to EU ministers for energy and environment meeting in Milan. Activists from Italy, Germany, France and Austria unfurled a banner reading “people want renewables and energy efficiency” as the ministers got out of their cars to enter the meeting. All five activists have been detained by the police but not charged. The banner was a sharp reminder that only a few weeks ago hundreds of thousands of people were on the streets urging leaders to address climate change.

Agribusiness

- Consumer Union published a study regarding GMO labeling costs. The study found that required GMO labeling would cost consumers a median of less than a penny per day ($2.30 per year). These findings refute claims by anti-Measure 92 and other anti-GMO labeling ad campaigns that GMO labeling would increase costs dramatically for consumers.

- Billion-dollar class action lawsuits have been filed by farmers and organizations in Iowa, Nebraska, and Illinois, claiming that Syngenta has damaged their profits and the corn market nationally by introducing MIR162 GM corn which has been rejected by China.

- According to Civil Beat, a new anti-GMO PAC has been formed. According to the article, the Center for Food Safety has formed the PAC called the Coalition for a Safer, Healthier Maui. The group will work to oppose already robust campaigns against Maui’s GMO moratorium, for example that of the group Citizens Against the Maui County Farming Ban.

- On October 8, 2014, Sustainable Pulse published an article about the biotech domination of African seed companies. The article discusses the strong concern on the Alliance for Food Sovereignty in Africa over multinational food companies acquiring Africa’s home-grown seed companies. The article mentions several large multinationals specifically including Groupe Limagrain from France and Mahyco from India which is 26% owned by Monsanto. Monsanto, Dow, and Syngenta are mentioned specifically as three of the largest biotech firms that now have a strong foothold in Africa in maize and cotton crops.

- As of October 10, 2014, a petition to the White House calling on President Obama to reject Dow Chemical’s 2,4-D resistant GE crops has collected the 100,000 signatures necessary to be delivered to the president. The petition was promoted by The Dr. Oz Show which aired segments of their weekly programming on GMO cultivation and the rising concern over related pesticide use.

- Start-up companies such as FarmLogs and 640 Labs are in the hunt for customers along with agribusiness giants Deere, Pioneer and Monsanto in the new agricultural field of Big Data.

- Genetically engineered crops get undue credit for reducing soil losses on cropland, says the Environmental Working Group. In a three-page analysis, EWG says the credit really should go to so-called conservation compliance and the Conservation Reserve, both created by the 1985 farm law.

- The Argentinian news portal Infobae says the government is considering whether to create a grain company of its own to compete with the multinational exporters - Cargill, ADM, Bunge and Dreyfus -who dominate farm exports. The goal would be to see that farmers sell their grain for higher prices, says the report, which describes the new company as a trial balloon.

- Class-action lawsuits asking $1 billion in damages from seed company Syngenta were filed in federal court in Iowa, Illinois and Nebraska. The lawsuits say growers and processors lost sales because Syngenta’s MIR 162 genetically engineered corn is not
approved for sale in China, which has rejected tens of thousands of tonnes of U.S. corn shipments on grounds they contain the Syngenta grain.

Insurance/Healthcare

- The Office of the National Coordinator for Health Information Technology (ONC) published an October report to Congress that provided an update on the adoption of health information technology. Through the lens of the electronic use and exchange of health information, the report touched upon evidence of progress of a nationwide system, adoption barriers, and specific federal actions to reduce those barriers.

- California Governor Edmund Brown Jr. recently signed into law a new measure that extends healthcare organizations’ breach notification deadline to 15 business days. Previously, medical facilities in the state had to notify breach victims and state officials within five business days of detecting a breach to comply with California Health & Safety Code 1280.15.

- The Health Information Trust Alliance, in collaboration with several healthcare-related organizations, has developed and is piloting an automated early warning system to share cyberthreat intelligence.

- Finding qualified healthcare security personnel remains a challenge in an industry where new threats make protecting patient data more complex by the day.

- Long on the periphery of the healthcare industry, social media networks are now coming into focus because of the growing interest in consumer health through mobile applications. A recent Reuters report discussed how Facebook is taking early steps toward forming online communities that would facilitate conversations between users with similar ailments and be geared toward preventative care.

- People who fake the thefts of their vehicles to collect insurance money usually never see the inside of a jail. A review of 133 cases since 2009 found that six of 10 people convicted don’t serve jail time for this crime. They're usually ordered to repay the insurance company and perform some community service. Of those who go to jail, the average sentence is just more than a year.

- The U.S. Food and Drug Administration (FDA) recently published new guidance aimed at helping medical device manufacturers manage cyber security risks.

- Federal authorities are ramping up efforts to crack down on healthcare fraud, announcing plans to prosecute top executives at hospitals and other organizations involved with fraud - and target other fraudsters as well.

- A few state representatives are trying to see to it that patients have more of a say over the privacy of their HealthCare.gov data. The new bill proposed by Reps. Robert Hurt, R-Charlottesville, and John Barrow, D-Ga., would allow patients who opt out of HealthCare.gov coverage to completely remove their permanent profiles.

- The American Health Information Management Association (AHIMA) recently published its Information Governance Principles for Healthcare (IGPHC). AHIMA determined that there are eight core principles involving data privacy and security for healthcare organizations to consider.

- The New Jersey Assembly passed a measure that would make reverse rate evasion an insurance fraud and provide for civil and criminal penalties. The bill, A 2281, passed the state’s Assembly in late September and is pending in the state Senate.
Financial Services

Activism

- A housing activist group urged their supporters to “pack the courtroom” in Chicago, IL during an eviction hearing on October 28th in support of a local homeowner facing eviction from a GSE for housing.

- Housing activists held a protest against the two GSEs for housing in Boston, MA on October 9th, condemning the two agencies’ efforts to get the Attorney General’s lawsuit dismissed. The Attorney General has sued the GSEs for violating state law when they refuse to sell homes to any non-profit that will sell back to former owners.

- Environmental activists will hold a protest in front of a leading U.S. bank in London, UK on October 28th, speaking out against the bank’s investments in biomass power stations in Avonmouth and Southampton, UK.

- A ‘March Against Corruption’ international campaign action will occur on November 1st at Zuccatti Park in NYC. The purpose of the campaign is to raise awareness about the corrupting influence of money and special interests in governance and public policy making.

- Housing activists will organize a “speak-out” event on tax foreclosure abuses and to build support for saving homes and neighborhoods on October 11th in Detroit, MI.

- An online petition calls for financial institutions to remove forced arbitration requirements from their contracts with customers. The petition claims forced arbitration functions as a “license to steal” and makes it impossible for customers to hold financial institutions accountable in court if they break the law. Several leading U.S banks are specifically named in the petition.

- A housing activist group will stage a ‘Nightmare from Wall Street’ action at a public Halloween event in Los Angeles, CA on October 31st, speaking out against multiple bank brands for their alleged corrupt housing operations.

- A coalition of activists is planning a “Ghosts of Wall Street educational spectacle” event during the New York City Halloween Parade on October 31st. The Ghost of Wall Street rally will gather at 5:00 PM EDT and a press conference will be staged at 6:30 PM EDT. Participants will address banks’ roles in foreclosures, rising rents, and “financial shenanigans.”

- Anarchists in Australia issued a call for decentralized attacks, disorder, riots and sabotage during the G20 Summit that will take place on November 15th through 16th in Brisbane, Australia.

- Occupy Wall Street encouraged supporters to call various members of the World Bank’s press office on Thursday, October 9th from 2:00pm to 4:00pm EDT in efforts to disrupt the bank’s operations during the lead up to their annual meeting in Washington, D.C. on Friday October 10th.

- A leading teachers’ pension fund management company was named as a target by labor activists who have been fighting against a multi-brand restaurant operator headquartered in Orlando. The activists held protests at the NYC and Philadelphia offices of the pension fund company on October 9th condemning their continued investments in the restaurant holding company.

- Occupy Los Angeles will host its Anniversary People’s Assembly in Solidarity Park in Los Angeles, CA on October 11th. The event will feature workshops, speeches, and performances that will focus on a variety of topics including anti-police brutality/spying
and home defense.

- An activist website offered $1,000,000 reward for information related to the government’s “lawless attempted seizure” of the two GSEs for housing. The website encourages former employees from the GSEs and the FHFA, and the Treasury Department to share information that would expose the government’s attempts to seize the GSEs. The website stated the reward may exceed $1,000,000.00, and that anonymity will be protected.

- Multiple posts on a popular micro blogging site claimed that a leading U.S. investment firm is spreading false financial data about the two of the biggest U.S. automakers.

- An activist group launched a boycott campaign directed at a leading U.S. fast food chain for the company’s pursuit of acquiring a Canadian restaurant chain, a move likely to reduce the U.S. fast food company’s tax obligations in the states. The campaign however is also critical of a leading U.S. investment firm, likely due to its recent upgrade and promotion of the fast food chain’s stock.

- A ‘Pack the Courts’ action for an arrested Occupy Wall Street activist occurred Friday, October 10th at the Manhattan Criminal Court in NYC. The OWS activist was arrested for filming police as they arrested two people in the Union Square subway station in December 2013.

- Protests occurred at the World Bank’s headquarters in Washington, DC on October 10th and 11th as protesters called for human rights before corporate profits.

**Information Security Risk**

- Hackers are promoting a hacking campaign dubbed '#OpRemember' to launch on November 5th that is set to target "the global banking cartels, the oil and gas industry, the corrupt governments of the world, the bio-tech industry, and the mega-corporations that control our planet." Individuals are encouraged to perpetrate an array of actions against targeted entities, including website dumping and defacing, as well as DDoSing, email hacking, and the Doxing of "corrupt bankers or government officials."

- Reports said the group of overseas hackers who recently infiltrated a leading U.S bank, also breached the systems of 13 other financial institutions. The hackers are thought to be operating from Russia and appear to have at least loose connections with officials of the Russian government.

- The director of the FBI warned that Chinese hackers embarked on a widespread campaign of cyberwarfare against the US, claiming "there are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese."

- A leading U.S. telecommunications company informed about 1,600 customers that an employee gained unauthorized access to their personal data in August. The company said the person may have obtained Social Security numbers, driver’s license numbers and services customers subscribed to. Federal authorities have been notified regarding the incident, and the employee has since been fired.

- A new study said Russian-speaking cybercrime groups are targeting primarily US-based systems and online banking accounts. Qbot (aka Qakbot) botnet of 500,000 infected systems sniffed ‘conversations,’ including account credentials, for 800,000 online banking transactions, with 59% of sniffed sessions representing accounts at five of the largest U.S. banks.

- A security researcher notified the nation’s largest bond insurer that a misconfiguration in one of the company Web servers had exposed countless customer account numbers, balances and other sensitive data. Much of the information had been indexed by search engines, including a page listing administrative credentials that attackers could use to access data that wasn’t already accessible via a simple Web search.
Researchers said they detected many automated teller machines infected with a newly
discovered ATM-specific malware, called Tyupkin. Once the malware has been
installed, the "mule" sent to collect the cash must enter a code on the machine's key
pad. But Tyupkin then requires a second unique code - randomly generated by an
algorithm at a remote location - to unlock the machine and dispense the cash. It is this
part of the process that ensures the criminal who has this algorithm retains control
over when and how often these illegal withdrawals occur.

A researcher claimed that an American software company known for the Portable
Document Format (PDF) is tracking users using their E-reader app and uploading the
data to their servers. The researcher said the company is gathering data on the
ebooks that have been opened, which pages were read, and in what order. All of this
data, including the title, publisher, and other metadata for the book is being sent to the
company’s server in clear text. The software company, according to the researcher, is
not only logging what users are doing, but also sending those logs to their servers in
such a way that anyone running one of the servers in between can listen in and know
everything.

A Minnesota-based national fast food chain confirmed that Backoff point-of-sale
malware was used in a payment card breach that affected 395 of its 4,500 franchised
U.S. locations. The company’s own investigation revealed that the breach stemmed
from a compromise of a third-party vendor’s account credentials, which the attackers
used to access systems at the affected locations across 46 states.

Security researchers discovered a watering-hole attack orchestrated by a cyber-
espionage dubbed Sednit that targets individuals connected to the military sector;
victims are redirected from the website of a large financial institution in Poland
(undisclosed) to defense-related domain names hosting an exploit kit. Sednit is known
for having conducted email-based targeted attacks in the past, using the spear-
phishing technique. The emails sent to the victims had an attachment with a malicious
Microsoft Word document and exploited a zero-day vulnerability in the software to
deliver a piece of malware. Recent observations from the security researchers showed
that the group added an iframe into the websites of the financial firm in Poland.

Legal, Litigation, Regulatory Risk

A senior U.S. Senator questioned the Treasury Department’s decision to award a
leading U.S bank an exclusive contract to provide technology and financial services in
all federal prisons. In a letter sent Friday, October 3rd, the Senator from Iowa asked
the Treasury how the deal can protect taxpayers from fraud and conflicts of interest,
given that it was awarded without the competitive bidding and transparency required
for most federal contracts. The Senator said in a statement to the Center for Public
Integrity, “any time the government avoids competitive bidding, the practice needs
exploration.” The Center first reported on October 2nd that the bank has been paid at
least $76.3 million dollars to manage inmates’ accounts and oversee e-messaging and
phone services inside the 121 facilities managed by the Bureau of Prisons, which
house more than 214,000 prisoners. The deal has been amended 22 times since it
was awarded in 2000. Treasury granted it under a 150-year-old authority that allows
the agency to sidestep the oversight, transparency and competition typically required
for federal contracting. The contracts are known as financial agency agreements.

The Justice Department is planning a new round of “attacks” on the world’s biggest
banks, again questioning Wall Street’s role in a broad array of financial markets. The
article added that there is mounting evidence that a number of foreign and American
banks colluded to alter the price of foreign currencies, and prosecutors are aiming to
file targets on at least one bank by the end of the year.

American and European banks are nearing settlements deals with British regulators for
allegations over “rigging interest rates and manipulating the foreign exchange market.”
The author wrote that the Britain’s Financial Conduct Authority is holding talks with
several leading U.S. banks on the Libor manipulation issue.

Operational Risk
The CEO of an American online retailer headquartered in Utah accused a leading US clearing and settlement Services Company of corruption, alleging that the corrupt system can be fixed by using cryptocurrencies, bypassing the stock market, and using his newly created peer-to-peer alternative to Wall Street.

An op-ed published last week said that the banking industry's lobbying of the Cybersecurity Information Sharing Act (CISA) bill raises concerns regarding citizen privacy. The piece alleged that banks desire the ability to share more customer data with the government and all the while desiring privacy when faced with the possibility of consumers' complaints about them going public.

Philippine authorities warned that criminals are stealing cash from ATMs by using Jackfruit sap daubed on a metal bar inserted into the card slot. Whenever a customer tried to withdraw cash, the bills would stick onto the bar inside of the machine, which thieves would retrieve once the disappointed customer left.

Financial market participants criticized plans for a New York-based stock exchange to begin monitoring itself through its non-profit division, describing the move as a "retrograde step" that will never work in practice. Despite the objections, the division insists that it can safely monitor and discipline the exchange without any help from the Financial Industry Regulatory Authority (FINRA).

**Reputational Risk**

An article published last week claimed that the Texas Attorney General allowed a leading U.S. bank to "walk away with millions of taxpayer money." The author called out the Attorney General for allegedly letting the bank, which happens to be one of his donors, walk away with $3.3 million dollars of taxpayer money from the Texas Enterprise Fund.

**Global Intelligence**

**China**

- Anonymous threatens China and Hong Kong authorities with blackout and followed-up on its threat, releasing data from mainland government websites. The hacktivist collective claimed that it infiltrated more than 50 mainland government databases and leaked thousands of usernames and emails.

- On 10/6/2014, Radio Free Asia reported an update on the pro-democracy protests in Hong Kong. Since Monday, the number of protesters shrank to just a few hundred, as many returned to work and school. The remaining protesters encamped outside central government headquarters in Hong Kong's Admiralty district made no attempt to obstruct government staff from entering the building to return to work.

- On 10/9/2014, PC World reported that on Wednesday, nearly 1,000 workers at Foxconn's Chongqing plant went on strike to demand higher wages, after production orders from Hewlett-Packard were cut. Allegedly, Foxconn had been reducing workers' overtime at the factory according to China Labor Watch. A Reuters report stated that workers returned to their jobs on Thursday and production at the plant was unaffected.

- On 10/9/2014, Reuters reported that Chinese Internet company Baidu signed an agreement on Thursday to acquire Brazilian group buying site, Peixe Urbano, Details regarding the price of the transaction were not released at the time.

**India**

- On 10/8/2014 The Economic Times reported that Yahoo has started to lay off workers in India as it seeks to consolidate its product engineering teams at its headquarters in Sunnyvale. Yahoo's India operations will be reduced to support and operation
functions. Yahoo India R&D head Hari Vasudev and a few other senior executives have been asked to move to the US. Amit Dayal, vice president of search and marketplaces, has already shifted there.

**North America**

- Social media app Snapchat was hacked, and more than 200,000 pictures were stolen. There is extra concern over the pictures due to the fact that 50% of its users range from 13 – 17 years old.

- On 10/7/2014 Forbes reported that the Supreme Court heard the case and decide on the question if Amazon workers should be paid for security screening. The decision will have serious ramifications for 76 million hourly workers. After clocking out at the end of a shift, Amazon workers had to pass through security checks before leaving the building to ensure they didn't steal anything from Amazon. The security screenings often involved waiting in long lines, sometimes taking half an hour to clear. Workers were not paid for the time they spent during security checks.

- On 10/7/2014 Yahoo!Finance reported that HP plan to lay off 55,000 workers in its move to split into two different companies. The 55,000 layoffs just announced by HP — about 18% of its global workforce of 300,000 or so -- exceed the total number of layoffs for all companies combined in every other month this year.

- On 10/7/2014 Yahoo!News reported that a huge reorganization of Cisco's routing and switching engineering business has been going on, affecting up to 25,000 employees. On 10/8/2014 Apple Insider reported that Apple and other tech companies have sent recruiters and other personnel to the three-day Grace Hopper of Women in Computing conference in an effort to bridge the Silicon Valley gender gap.

- On 10/8/2014 BGR reported that a day after Nokia announced its decision to suspend operations at its facility in Sriperumbudur, the employees' Union is looking at "legal options." Following the Nokia-Microsoft $7.2 billion deal, the voluntary retirement scheme was offered for employees and 5,700 of them opted for it, from the total of 6,600.

- A 10/10/2014 Facebook post by user "SEIU USSW " contains a photo of an SEIU USSW demonstration outside Google. SEIU stated that they encouraged tech companies to follow Google’s lead in parting ways with its security contractors. The incident also contains a petition addressed to Apple regarding this matter.

**Vietnam**

- On 10/2/2014 Market Watch reported that Samsung Electronics will invest $560 million to build a new plant the country to make TVs and other home appliances. The new factory will be built in a high-tech park in Ho Chi Minh City, Vietnam.

- On 10/3/2014 Reuters reported that growth in exports driven by manufacturing could give Vietnam a trade surplus of $1.5 billion this year, far surpassing its forecast of $500 million in July.

- On 10/6/2014 Tuoi Tre News, a local VNese media source, reported that Vietnam's suppliers have been unable to gain contract agreements with Samsung because they cannot ensure a competitive production cost of the supplies. The Vietnamese part suppliers make their products at high costs whereas their manufacturing capacity is low, thus failing to produce anything at competitive prices.

- On 10/6/2014 ChaoBuoiSang.Net, a local VNese media source, reported that several multi-national groups are eyeing Vietnam as the new production base. The article cited increase in productions by Nike, Adidas, Lancaster, Sequoia Paris, Intel, Samsung, and Nokia as few multi-national brands to shift their operations to Vietnam or increase their operations in Vietnam.

- On 10/9/2014 Info.VN, a local VNese media source, reported that Microsoft Devices Group will purchase phones from the Vietnam factory rather than the facility owned by
Nokia in Chennai.

Pinterest announced plans to make “Promoted Pins” available to more than just the handful of big brands that have been helping the company to test its ad product since last fall. The company expects to ultimately offer advertisers pay-per-click arrangements like the ones available to purchasers of Google’s sponsored search results, and is amending its privacy policy to state, among other things, that Pinterest may collect information about its users from its advertisers and in connection with its advertisers’ websites and apps.

The U.S. District Court for the Southern District of New York has found that setting up auto-forwarding to receive copies of another person’s incoming emails is a violation of the federal Wiretap Act.

Pharmaceuticals

- Drugmaker GlaxoSmithKline, which was slapped with a record $489 million fine for corruption in China last month, said on Tuesday it was looking into allegations of corruption in the United Arab Emirates. Britain's biggest pharmaceuticals group confirmed the investigation following allegations of improper payments set out in a whistleblower’s email sent to its top management on Monday.

Retail

- Daily Finance reported that ice cream and fast-food restaurant chain Dairy Queen has confirmed a security breach that may have compromised the payment card information of customers at several hundred locations across 46 US states. Computers at Dairy Queen locations were infected by Backoff malware.

- CNN Money reported that Wal-Mart is cutting health insurance benefits for nearly 30,000 part-time employees to control its rising health care costs. The cut applies to employees who work less than 30 hours per week.

- Twice reported that GameStop’s Spring Mobile wireless subsidiary has acquired 53 AT&T-branded stores from independent New York metro area chain Product Center. Spring Mobile now has nearly 300 AT&T-branded locations across 26 states.

- BBC News reported that UK supermarket giant Tesco has asked a fifth executive, commercial director Kevin Grace, to step aside, as the fall-out from its £250m profit forecast overstatement continues.

- Seattle Times reported that Redbox Instant movie-streaming venture between Outerwall and Verizon Communications ceased operations on Tuesday, Oct. 7, according to a notice to customers on its website.

Technology

- Android’s Cyanogenmod contains a zero-day vulnerability which can be used to execute man-in-the-middle attack due to a flawed code reuse.

- Variant of the Rovnix malware has additional features including a new domain generation algorithm and secure transmission channel for communicating with command-and-control servers.
Trend Micro Incorporated reports that the Kingdom of Saudi Arabia and UAE maintains the highest levels of malware detection in the Middle East over the past year.

Telecommunications

- Internet service providers in Denmark have reached an agreement with a leading anti-piracy group, Rights Alliance. Rights Alliance will only need to obtain a single pirate site blocking order against one ISP and all the rest will voluntarily block the same domains. While the entertainment industries are capable of obtaining blocking injunctions against pirate sites, each action has to be targeted at a specific service provider. That means rival ISPs are free to carry on providing access while an injunction might be issued against one ISP.

Defense

- Taiwan’s premier warns of increasing cyber-attacks from China are growing. The warning comes after the FBI warned that China is waging cyber-war against the United States.
- The Massachusetts Maritime Academy website was hacked twice last Monday in a cyber-attack that appeared to stem from an Islamic extremist group.
- The Electronic Frontier Foundation (EFF) has launched a new site dedicated to anti-surveillance by educating users on how to resist pervasive surveillance online.

Law Enforcement

- Crime fighting in the city of Tampa, Florida has been aided recently with the implementation of SAFE COP, a program developed by Assistant Chief John Bennett using technology from several sources. The SAFE COP — which stands for Situational Awareness for Enforcer’s Common Operating Picture, involves: Redistribution of Tactical Resources, Intelligence-led Policing, Proactive and Preventative Policing Initiatives, and Partnering with the Community.
- The use of Global Positioning Systems (GPS) jammers by criminals to thwart law enforcement response and investigation into cargo thefts in the United States has seen an increase lately. Since at least February 2012, various law enforcement and private sector partners have reported that GPS tracking devices have been jammed by criminals engaged in nefarious activity including cargo theft and illicit shipping of goods. Although banned by federal law, the jammers are readily available over the Internet and easy to employ.
- The Justice Department is mulling whether to investigate NYPD’s use of the controversial crime fighting strategy known as “broken windows.” The Justice Department Civil Rights Division is considering a request from six members of Congress to investigate whether black people and Hispanics are disproportionately affected by quality-of-life violations.