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 /Pharmaceutical
- Financial Services
- Global Intelligence
- Legal and Regulations

New White Paper: Social engineering in a Web 2.0 world has evolved to a fine art, characterized by highly targeted, customized attacks. Download this whitepaper to learn more about what steps you can take to protect your organization.

Top Incidents

Energy

- Hundreds of protesters marched Sunday in Washington, D.C., to show their opposition to a planned natural gas export terminal in Maryland that would ship gas fracked in the United States overseas to Asia. The Stop Fracked Gas Exports rally, backed by more than 40 environmental groups, called on the U.S. Department of Energy and the Federal Energy Regulations Committee (FERC) to halt final approval of a port they say will
endanger local health and safety.

**Agribusiness**

- Food and beverage companies have been a particularly hot target for activists on social media, since the uproar over lean finely textured beef AKA pink slime. Three of the top seven most popular petitions of all time on Change.org are about animal welfare in meat production, and more than two dozen food-related petitions have each earned tens of thousands of signatures, many of them hundreds of thousands.

**Insurance/Healthcare/Pharmaceutical**

- Investigators are taking drones to new heights — using the remote-controlled aircraft to catch New Yorkers lying about disabilities. Olwyn Triggs, president of Professional Investigators Network Inc., recently used a drone to find an upstate New York man suspected of insurance fraud. Signs on his rural property warned that trespassers would be shot, so she sent in her 2-pound, foot-long Phantom 2 Vision quadcopter to confirm the man wasn’t fully disabled as claimed.

**Financial Services**

- Researchers said the first half of 2014 has seen the largest number of volumetric DDoS attacks over 100Gbps ever, although the average size has reduced since the first quarter. The researchers gathered data from over 290 ISPs and discovered 111 DDoS events over 100Gbps in the first six months of the year. The data also revealed that already this year the number of attacks over 20Gbps has more than doubled the 2,573 events reported in the whole of 2013. Attack duration is also up – from 54 minutes on average in Q1 to 98 minutes in Q2, for attacks over 10Gbps. In terms of attack sources, South Korea was in the lead accounting for 15.1% - a rise of 2.6% since Q1 – with the US close behind with a 14.8% share, up 3.8% since the first three months of the year. China was next, accounting for 6.7% of DDoS attacks seen, an increase of 2.8% since Q1 2014.

**Global Intelligence**

- 7/10/2014 - Samsung is being pressured by labor activist groups such as Green America to cease alleged child labor abuses at its cell phone supplier factory in China. Green America has issued a petition, following a recent labor abuses report published by China Labor Watch.

**Legal and Regulations**


**Energy**

- The Green Alliance to Stop Pipelines reports that pipeline resistance is growing in New York State—Spectra faces stronger opposition as more people learn about the pipeline expansion. Carl Lundgren says, “The biggest concern is that the proposed Algonquin pipeline extension would be built over the active Ramapo fault line, not far from the Indian Point nuclear power facility. Members of groups such as Shut Down Indian Point Now! NYC (SDIPN) and Stop the Algonquin Pipeline Extension (SAPE) are working in coalition to publicize and stop these environmental disasters in the making.”
• Hundreds of protesters marched Sunday in Washington, D.C., to show their opposition to a planned natural gas export terminal in Maryland that would ship gas fracked in the United States overseas to Asia. The Stop Fracked Gas Exports rally, backed by more than 40 environmental groups, called on the U.S. Department of Energy and the Federal Energy Regulations Committee (FERC) to halt final approval of a port they say will endanger local health and safety.

• The Federal Energy Regulatory Commission rejected as inadequate parts of a proposal to beef up the security of the electric grid and sent the plan back for revision to the utility-dominated group that wrote it. In an unusual move for the agency, FERC on Thursday told the group, the North American Electric Reliability Corp., that it should correct some weaknesses in its proposed plan. The commission told the group to consider broadening the definition of equipment and facilities deserving protection and asked it to allow the federal government to designate additional facilities eligible for increased security. The commission tentatively accepted other provisions pending further analysis and public comment. FERC’s request could result in protective measures for a greater number of substations and, potentially, other facilities.

• The United States endures more blackouts than any other developed nation as the number of U.S. power outages lasting more than an hour have increased steadily for the past decade, according to federal databases at the Department of Energy (DOE) and the North American Electric Reliability Corp. (NERC). According to federal data, the U.S. electric grid loses power 285 percent more often than in 1984, when the data collection effort on blackouts began. That’s costing American businesses as much as $150 billion per year, the DOE reported, with weather-related disruptions costing the most per event.

• A group of firefighters in New Jersey have filed a lawsuit against their county government and multiple railroads, alleging negligent hazmat response, equipment and preparation in a 2012 derailment and vinyl chloride spill.

• The group Don’t Frack Ohio is planning an anti-fracking rally at the Ohio Statehouse in Columbus on August 20.

• Bradford County, PA’s Commissioners have requested that the Department of Justice investigate Chesapeake Energy. The Commissioners are concerned that Chesapeake’s post-production costs are eating into constituents’ royalty payments. This incident appears to be the latest in an emerging trend where local politicians or activists, unsatisfied with regulation at the state level, appeal to federal authorities for action against energy companies.

• Activists opposed to oil refineries and pipelines will be hosting a massive rally at the Kinder Morgan Railyard in Richmond, CA on August 9. The location was chosen because the region hosts several oil refineries, and the rail yard specifically is seeking to expand its capacity for handling oil trains.

• California officials have ordered an emergency shut-down of 11 oil and gas waste injection sites and a review more than 100 others in the state’s drought-wracked Central Valley out of fear that companies may have been pumping fracking fluids and other toxic waste into drinking water aquifers there.

• A new study released last week found higher than normal levels of pollutants in wild foods that comprise a large part of traditional Native American (First Nations) diets in Alberta, Canada. The study points the finger at the province’s large scale oil sands development in northeast Alberta.

• The Globe and Mail reports that TransCanada Corp. and partner Phoenix Energy Holdings Ltd., are proposing to build the $3-billion Grand Rapids pipeline that would transport 900,000 barrels a day of blended bitumen from Fort McMurray to the Edmonton area. But the project, which is now being reviewed by provincial regulators, is under fire from landowners, environmentalists and the Athabasca Chipewyan First
Nation (ACFN) who complain it is being fast-tracked without proper environmental assessment.

Agribusiness

- According to a joint scientific report by the environmental agencies of Austria and Switzerland and the German nature conservation agency, BfN, high levels of herbicide and pesticide use, often driven by GE crops, are destroying biodiversity. The report finds that the recent steady climb in herbicide use is due to an increase in weeds and other plant species developing resistance to the herbicides used.

- The Center for Food Safety (CFS) reports that the US Fish and Wildlife Service (FWS) has announced they will limit the use of neonicotinoid chemicals in all wildlife refuges in the Pacific region, including in Hawaii and other Pacific Islands, Idaho, Oregon, and Washington. The decision by FWS comes after a petition was delivered from CFS and acknowledgement of damaging effects the chemicals have on pollinators. The phase out is scheduled to take effect in 2016.

- Newcastle University in the UK announced that an international team of experts from Newcastle University has published the largest study of its kind on the difference between organic and non-organic foods. The study finds that there is a substantial difference in the nutrition between organic crops and conventionally grown ones. The find that organic crops are up to 69% higher in the number of key antioxidants. The study was published in the British Journal of Nutrition on July 11, 2014.

- Food and beverage companies have been a particularly hot target for activists on social media, since the uproar over lean finely textured beef AKA pink slime. Three of the top seven most popular petitions of all time on Change.org are about animal welfare in meat production, and more than two dozen food-related petitions have each earned tens of thousands of signatures, many of them hundreds of thousands.

- The Agriculture Department announced $9.7 million in emergency water assistance grants for 25 rural communities in California, now in its third year of drought.

- An Agriculture Department poultry lab mistakenly was sent a shipment that included the virulent H5N1 avian influenza virus by the federal agency now under scrutiny for sloppy procedures. The incident, which occurred in late March, was not reported to top officials at the Centers for Disease Control until last week.

- China will harvest a record 222 million tonnes of corn this year, an increase of nearly 2 percent from 2013, the Agriculture Department estimated. The larger crop would stem from larger plantings, up 1.3 percent from last year’s record 36.3 million hectares.

- The years-long fight between farm organizations and animal rights activists over laws prohibiting secretly filmed documentation of animal abuse is moving from state legislatures to federal courts as laws in Utah and Idaho face constitutional challenges.

- State rural crime investigators, ranchers and agriculture officials say they suspect rising prices for cattle and beef as likely factors in livestock thefts in Alabama and elsewhere.

- Grain markets reacted dramatically to the Malaysian plane crash in Ukraine.

- News outlets reported that the advocacy group MoveOn.org contributed $53,000 this week to defend Vermont in the lawsuit between the State of Vermont and members of the Grocery Manufacturer’s Association, an organization of over 300 companies in the
food industry.

Insurance/Healthcare/Pharmaceutical

**Insurance**

- Cybersecurity experts see famous data breaches, such as the massive Target incident last year, as precursors to what may lie ahead in healthcare. However, to a degree, medical identity theft is already a major concern in healthcare.

- Investigators are taking drones to new heights — using the remote-controlled aircraft to catch New Yorkers lying about disabilities. Olwyn Triggs, president of Professional Investigators Network Inc., recently used a drone to find an upstate New York man suspected of insurance fraud. Signs on his rural property warned that trespassers would be shot, so she sent in her 2-pound, foot-long Phantom 2 Vision quadcopter to confirm the man wasn’t fully disabled as claimed.

- The Information Commissioner’s Office (ICO) has found Betsi Cadwaladr University Health Board in breach of the Data Protection Act after sensitive information was sent to the wrong address. The information was disclosed when eight letters about patients were sent to one of the people affected in July 2013. Six of the letters included sensitive medical information relating to the patients’ treatment.

- There has been a major privacy breach in BC’s prescription medication dispensing information system, resulting in about 1,600 people’s personal information being accessed. The breach happened sometime between March 9th and June 19th of this year, when someone used a doctor’s PharmaNet account without the doctor’s knowledge. The information that was accessed included the names, dates of birth, addresses, phone numbers, and personal health numbers for all of the affected people.

- The Baltimore Regional Benefit Office is reorganizing after what appears to be a privacy breach. A Baltimore employee of the benefits division was found with thousands of claims documents stacked in his office. Management began sorting the documents and claim folders to determine which contain Social Security and other sensitive information and has directed audits of all staff office space.

- According to a news release from the U.S. Department of Veterans Affairs, an informational letter regarding the opening of the Minneapolis VA Community-Based Outpatient Clinic (CBOC) in Shakopee was recently mailed to 500 veterans with the name and address of a different veteran inadvertently duplexed, or printed, onto the back side of the letter. The Minneapolis VA is investigating how the duplication error occurred.

- If New York State is illustrative of a national trend, hacking poses a greater threat to businesses and other organizations than other types of data breaches. External cyber-attacks represent 40 percent of the nearly 5,000 breaches recorded in the state from 2006 through 2013; healthcare is the sector with the largest number of records exposed since 2006, at more than 1 million.

- Recent court dismissals of two class action lawsuits related to an Advocate Health Care 2013 data breach impacting 4 million individuals are a reminder of how difficult it can be for plaintiffs to prevail in cases where there is no evidence of damages, such as fraud or identity theft.

- A Department of Health and Human Services (HHS) Office of Inspector General (OIG) audit found some high-risk security vulnerabilities within New Mexico’s health insurance exchange. The OIG audit report hasn’t been released yet because of the sensitive
nature of the material, but records indicate the security gaps are serious in nature and have potentially left patient data out in the open for a long time.

- When much of a healthcare organization’s growth is derived from acquisition, there are undoubtedly a lot of moving parts. As the parent organization takes on new hospitals or practices, it must ensure that its IT and business strategies are implemented within the recent acquisitions.

- A medical center that kept sensitive health records of nearly 1,000 patients in a garden shed on a disused property has been reprimanded for breaching privacy laws. Boxes of records containing the personal details of patients were discovered at the Narre Warren South site when the shed at the Amberley Park Drive property was broken into in November 2013. Australian Privacy Commissioner Timothy Pilgrim investigated and found the medical center that owned the property had breached the Privacy Act by failing to properly secure the information.

- Blue Shield of California and the California Department of Managed Health Care (DMHC) announced that they inadvertently distributed 18,000 doctors’ Social Security numbers. Blue Shield mistakenly sent rosters to DMHC that mistakenly included the Social Security numbers, and DMHC failed to catch the error. The rosters also contained providers’ names, business addresses, business telephone numbers, medical groups, and practice areas.

- Bay Area Pain Medical Associates in Sausalito, California has been notifying patients of breach it experienced on May 19, 2014, when their office was burglarized and three desktop computers were stolen.

- Rady Children’s Hospital of San Diego suffered a human error-based data breach in June that affected 14,121 patients; the hospital’s administrators have since reported some steps taken to prevent a future occurrence.

- A breach of unsecured private health information involving more than 500 people last month has been remedied. Apple Valley Christian Care Center administrators say they notified those affected by the breach of confidential medical information through the center’s website. They said the compromised information about clients and family members varied widely, including name; Social Security number; date of birth; home address; dates of stay; Medi-Cal ID number, Medicare ID number, and/or other insurance information; information regarding Medi-Cal appeals; diagnosis codes; treatment information and medical history.

- Penn Medicine Tuesday announced a data breach involving receipts from Penn Medicine Rittenhouse that were stolen last month from a locked office in Pennsylvania Hospital. Notifications of the theft were sent to 661 patients Monday.

**Pharmaceutical**

- A federal grand jury indicted shipping company FedEx Thursday on charges of shipping prescription drugs for illegal online pharmacies. Prosecutors say that Congress, the Drug Enforcement Administration and other federal agencies warned FedEx for nearly a decade that their shipping services were being used to illegally distribute drugs like oxycodone and hydrocodone. However, prosecutors say, the largest cargo company in the world ignored the notices.

- Activists with the Gateway to Hell Campaign held an international week of action in which group members protested primate cargo for research purposes by Air France and KLM airlines. The majority of actions were held in airport terminals across Europe.

- The Financial Times revealed this week that GlaxoSmithKline admitted to bribery problems in its China business as long ago as 2001. About 30 people were sacked over allegations that doctors and health officials were given payments to push GSK products.
The cases are similar to the present bribery inquiry the business is facing.

Financial

Activism

- Housing activists held an anti-eviction protest at a district court in Detroit, MI on July 18th. Activists urged supporters to call the Chicago office of a government sponsored enterprise for housing and demand it let a local resident stay in her foreclosed property.

- Housing activists threatened that actions against the Federal Housing Finance Agency (FHFA) Director will escalate throughout the summer and fall.

- A protest against “The Global 1%” will occur October 7th at the World Business Forum in NYC.

- Occupy Wall Street hosted a ‘Strategic Planning Assembly’ on July 18th at Zuccotti Park in New York City to plan for upcoming actions around the city as well as the Third Year Anniversary of Occupy Wall Street on September 17th, and the World Business Forum on October 7-8th in New York City.

- Housing activists will hold an anti-eviction protest on August 1st at the State Capitol in Sacramento, CA.

- Housing activists held an anti-eviction protest on July 16th at the Dekalb County Sheriff’s Office in Decatur, GA.

- Housing activists launched a six-day eviction blockade on July 17th in support of a local family facing eviction from their home in Seattle, WA.

- An LGBT activist group urged supporters to boycott a leading U.S. bank following claims the bank asked employees if they were “an ally of the LGBT community.”

Information Security Risk

- Researchers said malware developers are advertising a new banking Trojan dubbed ‘Kronos’ on a Russian cybercrime forum at a cost of $7,000. The malware creators however are giving potential customers the opportunity to conduct one-week tests for the price of $1,000, which includes full access to the command & control (C&C) server and to all of the Trojan’s capabilities. The creators of Kronos promise a lifetime product license, and free updates and bug fixes for those who pay the $7,000, amount which can be paid via Bitcoin, Perfect Money, WMZ, and the Bitcoin/Litecoin exchange BTC-E. Similar to other banking Trojans, Kronos comes with form-grabbing and HTML injection capabilities that are allegedly compatible with both the latest and most older versions of Chrome, Firefox and Internet Explorer Web browsers.

- Various hacker groups claimed to have taken down the websites of several leading Israeli banks as part of the anti-Israel campaigns, #OpSaveGaza and #OpIsrael.

- Hackers breached the databases of a regional bank in southern Florida and may have obtained access to personal information that includes customer names, addresses, account numbers, account balances, and personal identification numbers (for example, social security number, driver's license number, passport number, alien registration number).

- A new banking Trojan, Win32/Aibatook, is spreading through compromised Japanese pornography sites. The malware targets users of Internet Explorer who are customers of Japanese banks, and in particular visitors to some of the country’s most popular
pornographic websites. Users visiting any of the compromised sites can be redirected to an exploit page that attempts to take advantage of Java vulnerability CVE-2013-2465 which was patched in June 2013. If a vulnerable Windows computer is identified, a 404 error page is displayed to mask that the PC is silently running a malicious Java applet.

- Researchers said the first half of 2014 has seen the largest number of volumetric DDoS attacks over 100Gbps ever, although the average size has reduced since the first quarter. The researchers gathered data from over 290 ISPs and discovered 111 DDoS events over 100Gbps in the first six months of the year. The data also revealed that already this year the number of attacks over 20Gbps has more than doubled the 2,573 events reported in the whole of 2013. Attack duration is also up – from 54 minutes on average in Q1 to 98 minutes in Q2, for attacks over 10Gbps. In terms of attack sources, South Korea was in the lead accounting for 15.1% - a rise of 2.6% since Q1 – with the US close behind with a 14.8% share, up 3.8% since the first three months of the year. China was next, accounting for 6.7% of DDoS attacks seen, an increase of 2.8% since Q1 2014.

- The infamous banking Trojan called ‘Neverquest’ or Trojan.Snifula has been increasingly targeting users in Japan, Germany, and the United States. The malware is known to be continuously evolving and developing new features to steal more confidential online banking information. Snifula includes many features for stealing confidential information from compromised computers including, keystroke logging, screenshot and video capture, remote control, stored user name and password extraction, digital certificate theft, man-in-the-browser (MitB) attacks. Once Snifula has infected a computer, it downloads a configuration file from a command-and-control (C&C) server. The configuration file is specifically crafted for each target.

- The Federal Bureau of Investigation said criminals are developing increasingly sophisticated attack strategies that let them infect as many as 18 systems per second with their botnet armies. The botnets have caused over $9bn in losses to US victims and over $110bn in losses globally, and approximately 500 million computers are infected globally each year. Further, many of the botnets are currently rentable and could be used by a variety of criminals or terrorist organizations.

**Legal, Litigation, Regulatory Risk**

- An article published last week on a website frequented by fund managers, chief operating officers, risk managers and operational due diligence employees at buy-side firms called for more effective enforcement of pre-existing regulations as opposed to enhanced regulation of dark pools and HFTs to solve the challenges facing these organizations.

- The Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) announced that a former employee of a government sponsored enterprise for housing has pled guilty to engaging in unauthorized access to government servers that hosted a website used to support federal mortgage loan modification programs, including the Home Affordable Modification Program (HAMP).

- Federal authorities announced the successful prosecution of yet another member of an international cybercrime ring that’s been tied to a global ATM cash-out scheme. This time, the scheme was linked to the exploitation of prepaid cards provided by an American humanitarian organization to disaster relief victims after the network hack of a payments processor used by the charity.

- The Department of Justice filed a status update with a federal court in Pennsylvania, telling the judge that both the Gameover Zeus botnet and Cryptolocker "remained neutralized." Cryptolocker, which is a type of "ransomware" or extortion malware that encrypts files and then tries to convince users to pay to have them decrypted, was distributed exclusively by Gameover Zeus. The disruption of the original Gameover Zeus, and cleanup efforts by various countries’ computer security response teams, or
CIRTs, and Internet service providers, have reduced the number of infected PCs by more than 31%, the DOJ said in the report.

- The head of the Justice Department's criminal division told a Senate subcommittee on July 15th that Congress must update U.S. anti-hacking laws to allow law enforcement agencies to more easily crack down on fraudsters operating abroad, disrupt botnets used to distribute spam and distributed-denial-of-service attacks and bust “for hire” malware and botnet service providers.

- Romanian and French authorities dismantled a cyber criminal network that infected computers at money transfer outlets across Europe and used them to perform illegal transactions. The gang was also involved in the theft of credit card details through skimming, credit card cloning, money laundering and drug trafficking. The gang, which was composed mostly of Romanian citizens, infected computers at copy shops that also operated as money transfer franchises in Austria, Belgium, Germany, Norway, the U.K. and other European countries. No details were released about how the computers were infected, but Europol said that the attackers used a remote access Trojan (RAT) program.

**Operational Risk**

- According to a survey conducted by a leading security firm, in 2014, 52% of financial companies reimburse customer losses caused by Internet fraud without actually investigating the circumstances. Almost a third of companies believe the costs incurred by cyber threats are less than the cost of protection. The post warns as cyber criminals increasingly target e-payments, this approach could translate into considerable expenses for the company. Many organizations that work with online payments are prepared to accept the additional costs that arise from cyber-attacks. 28% of the representatives from financial companies and 32% of the online store employees polled are sure that the total losses from online crime, including reimbursement of stolen money, do not exceed the costs of deploying security solutions. Only 19% of financial companies and 7% of online marketplaces cite the cost of compensating customer losses in the top three most serious consequences of cyber fraud.

- A trade association representing service providers and suppliers in the telecom industry warned consumers about an increase in the number of scams that rely on caller ID spoofing. According to the organization, one tactic used by sales people and fraudsters attempting to collect personal information is that they make calls that appear to come from the recipient's own number. Those who have caller ID services usually pick up the phone out of curiosity.

- New research released on Wednesday (July 16) found that 72 percent of fraud victims in the Chicago area were also victims of data breach, suggesting a strong link between breaches and fraud.

**Reputational Risk**

- A Salt Lake City news outlet claims then-Attorney General Mark Shurtleff interviewed for a job with a law firm that represents a leading U.S. bank just two months before he personally signed a settlement of a lawsuit against the financial institution over whether it was illegally foreclosing on homes in Utah, which resulted in his hiring.

- An article published last week said that an American company that provides software for organizations to use on-premises or as part of cloud computing environments alleged in a recent lawsuit that a leading U.S. bank illegally copied $300 million worth of its enterprise software for use in a massive IT project at its subsidiary company while it was still within the terms of a license agreement prior to it expiring in February 2013.

- A petition launched by a local resident in St. Louis, MO claimed that she was evicted from their home because a leading U.S. bank refused to work out a new payment plan
Global Intelligence

Bolivia

- On July 17, 2014 Bolivia passed a law lowering the working age from 14 to 10; making the country the first nation to legalize working at the age of 10. Under the legislation, 10-year-olds will be able to work as long as they are under parental supervision and also attend school. It sets 12 as the minimum age for a child to work under contract.

China

- On 7/18/2014, a Chinese news outlet reports the number of cases of 20 Gbps DDoS attacks doubled and there are more than 100 cases of DDoS attacks that exceed 100Gbps, over the first half of the year.

- 7/10/2014 - Samsung is being pressured by labor activist groups such as Green America to cease alleged child labor abuses at its cell phone supplier factory in China. Green America has issued a petition, following a recent labor abuses report published by China Labor Watch.

- On 7/17/2014, a Chinese news outlet reports a survey shows there are 890482 fake application, and among 394263 of them are malwares and 59185 built-in with aggressive adware.

- 7/17/2014 - A recently laid-off female worker reportedly jumped to her death from the top of a four-story building at a footwear supplier factory in Shenzhen. Starting in May, employees, who feared being laid off without proper compensation, have been involved in a labor strike after the factory was ordered to undergo upgrades and legal changes by the local government. The factory supplied footwear globally for brands such as M&S, Clarks, and Pacific Brands.

- On 7/16/2014, a Chinese news outlet reports a group in Chongqing, China arrested for stealing 30,000 QQ account login credential through implanting malicious trojan and cashed out Q coins within the accounts.

- On 7/16/2014, a Chinese technology news outlet reports Windows Phone 8.1 contains a security vulnerability that affect users with Enterprise version.

- 7/18/2014 - Digitimes reported that Foxconn is recruiting 100,000 production line workers at its factory in Zhengzhou (Henan Province). The workforce will mainly produce iPhones for Apple, according to sources.

- On 7/16/2014, a Chinese news outlet reports Riot Game server were breached twice, and later found out that the attack was from an Australian with Asperger Syndrome. The hacker breach Riot Game server, obtain League of Legends' players information and sold the information.

- On 7/16/2014, a Chinese technology news outlet reports Facebook's SDK contains vulnerability that could expose million of mobile device users Facebook authentication login.

- On 7/13/2014, a Chinese news outlet reports a recent discovery of the variants of malicious trojan called Trojan_Generis.DP. The variants spread via removable storage media, the infected machine is not able to run safe mode normally for system repair.
On 7/14/2014, a user named “btcshop” posted on a Chinese forums reporting Mintpal website experienced a hacker attack and lost massive amount of virtual currency (VeriCoin).

Malaysia:

• On 7/13/2014, MTUC posted a blog posting regarding MTUC claimed that a multinational electronics company is utilizing outsourcing agent to employ foreign worker. The name of the electronics company was not mentioned in the blog posting and the company has denied the accusation.

• On 7/15/2014, a Malaysian news outlet reports boycotting products associate with Israel will effect Malaysians but not Israel. The article contains commentaries from other users but they did not mention anything regarding Intel.

• On 7/13/2014, a Malaysian news outlet reports calls on boycotting Israel products but not Jewish products.

• On 7/15/2014, a news outlet reports MTUC calls on the government to implement a five-day work week in private sector to increase productivity.

• On 7/10/2014, a Malaysian news outlet reports dengue cases in Malaysia have reached endemic level and encourage the public to clean up Aedes mosquitoes breeding spot.

North America

• Microsoft has posted a request form to block Bing search results in Europe. The form is posted in a response to the decision by the European Court of Justice regarding the Right to Be Forgotten (Google v AEPD, Gonzalez). Google posted its form a few weeks ago and received tens of thousands of requests within the first few days. Interestingly enough, the form reflects on the many questions around this judgment and the lack of guidance. Therefore, Microsoft will review the form and related processes as additional guidance becomes available and submissions may be reevaluated.

• The Senate Intelligence Committee will vote on a cybersecurity bill that will allow companies to share digital information about threats. Privacy advocates fear this could endanger net neutrality and boost surveillance efforts. The bill lacks a clause that states nothing in the legislation could “limit liability for actions that would violate the regulations adopted by the Federal Communications Commission on preserving the open Internet, or any successor regulations.”

• Thread Group, a network technology firm presents a network protocol that can help the communication of the Internet of Things. With Thread, product developers and consumers can securely connect more than 250 devices into a low-power, wireless mesh network that also includes direct Internet and cloud access for every device.

• The USTelecom has warned consumers about an increase in the number of scams that rely on caller ID spoofing. Pindrop Security, a company that specializes in phone fraud protection solutions, confirmed for SecurityWeek that the volume of attacks on consumers is increasing, and also pointed out that caller ID spoofing and other obfuscation is widely used in attacks on businesses as well.

• According to the recent survey on the Internet of Things called “Spiceworks survey 440 IT pros”, 71% of IT professionals know that the IoT will affect both consumers and the workplace, but less than half are doing anything with that knowledge. Then there are the security and privacy issues surrounding the IoT, which concerns 86% of respondents. An indication that many tech professionals are hoping the IoT can be kept at bay is that, according to the Spiceworks survey, 43% plan to relegate new Internet-enabled "things" to a separate network; only 23% plan to allow them on the corporate network.
The FTC and DOJ recently issued their annual merger report, reviewing their key merger enforcement actions during 2013. The report is a goldmine of useful information for companies seeking to evaluate their business strategies and comply with the regulators.

On July 15, 2014, the Internal Revenue Service released T.D. 9676, the final rules on the allocation and apportionment of interest expense by corporations owning a 10% or higher interest in a partnership.


On July 11, 2014, the FCC adopted a Second Order on Reconsideration and Second Further Notice of Proposed Rulemaking responding to a coalition of consumer groups that had pushed the FCC to reconsider its position and require that programming distributors (broadcast, cable, and satellite) include closed captioning for certain IP-delivered video clips. The new rules will apply to video clips only if the video clip was shown on television and then posted online to the programming distributor’s own website or mobile app and do not apply to consumer-generated media. The Order sets forth a number of compliance deadlines.

A number of amendments to Delaware General Corporation Law (“DGCL”) Section 251(h) have been passed by the Delaware legislature, clarifying a number of issues that have arisen since adoption of the law last year. If signed by the Governor (as is expected), the amendments will apply to merger agreements entered into on or after August 1, 2014. Under Section 251(h), a merger agreement can include a provision that eliminates the need for a target stockholder vote for a merger after a tender or exchange offer if, among other conditions, the acquiror then owns at least the number of shares that would be sufficient to approve the merger under the DGCL and the target’s charter.

Effective July 1, 2014, Florida has a new data breach notification law (S. 1524) that adds significant new requirements for companies that suffer breaches. Among other things, the law adds to the definition of “personal information” medical and health insurance data and information that permits access to a person’s online account. It also shortens the period in which notification must be made to 30 days (from 45) and requires that the Department of Legal Affairs be notified whenever a breach affects 500 or more Florida residents. Moreover, the new law requires businesses to “take reasonable measures” to protect personal information in electronic form.

On July 15, 2014, the UK Information Commissioner’s Office (“ICO”) released its Annual Report for 2013/14 (the “Report”). Entitled Effective, Efficient – and Busier than Ever, the Report illustrates the rapid growth of data protection and freedom of information issues in the UK in the past year. It highlights the fact that the ICO has received increasing numbers of questions and complaints from members of the public, processed record numbers of cases, and issued its highest ever level of fines, totaling almost £1.97 million.