Welcome to the Cyveillance Weekly Trends Report

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

In this Issue:

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

Join Cyveillance and Centripetal Networks as we explore the challenges in closing the breach detection gap, managing large dynamic sets of threat intelligence, and how to operationalize threat intelligence in a perimeter defense strategy.

Date: April 9, 2015
Time: 1:00 PM ET

Top Incidents

Energy

- Snohomish County (WA State) Train Watch is soliciting volunteers to identify, track and document train traffic passing through the county during the week of April 19-25. The group is specifically concerned about oil trains, and claims to be planning to hand the gathered data to local officials and emergency responders.

Agribusiness

- The FBI has invoked the broader powers afforded by the Foreign Intelligence Surveillance Act, or FISA, to surreptitiously gather evidence against two Chinese siblings accused of plotting to steal patented seed from Iowa cornfields, according to court records. Stealing hybrid seeds enhanced with traits such as drought resistance doesn't pose the same immediate threat as a suicide bomber, but the FBI treats economic espionage and similar trade secret theft as dangerous threats to national security.
security.

**Insurance/Healthcare**

- As more mega-breaches occur, cyber-insurers will more closely assess the security risks of potential clients, leading more organizations to improve their information security programs, attorney John Yanchunis predicts. “When companies are unable to get insurance ... you’re going to see companies adopting better security systems,” says Yanchunis of the Florida-based law firm Morgan & Morgan, who’s representing consumers in several breach-related lawsuits. Those cases include one of the class action suits filed against Premera Blue Cross in the wake of a hacking incident that affected 11 million individuals.

**Financial Services**

- President Barack Obama signed an Executive Order on Wednesday, April 1 allowing the use of economic sanctions for the first time against perpetrators of destructive cyber-attacks and online corporate espionage. The move will let the Treasury Department freeze the assets of overseas individuals and entities identified as the source of cybercrimes. The federal government also will be able to bar U.S. citizens and companies from doing business with those targeted for sanctions.

**Global Intelligence**

- A forum post on Bitcointalk.org reports a Chinese bitcoin trading network, BtcTrade, suffered multiple DDoS attacks since March 26. According to the post, the attacks stopped on March 30th but the network has not returned to normal yet.

**Legal and Regulations**

- In an attempt to verify compliance with the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule, the Office of Civil Rights (OCR) for the United States Department of Health and Human Services piloted privacy and security audits of covered entities in 2011 and 2012 (the “Phase 1 Audits”). Phase 2 Audits will likely begin soon. In the meantime, covered entities and business entities should take advantage of the delay by reviewing their current HIPAA compliance programs.

**Pharmaceuticals**

- A campaign to reduce the use of animals for medical research in the U.K. is causing howls of protest from scientists who say such a move would effectively ban nearly 89% of research that is conducted. The campaign was started recently by the British Union for the Abolition of Vivisection. The advocacy group, which wants to end all animal experiments, asked members of the U.K. parliament, as well as candidates running for seats in the governing body in upcoming May 7 election, to sign a six-point pledge to curtail the use of animal in medical research.

**Retail**

- Online retailers battling with fraud prevention are losing out on genuine sales by treating their customers like criminals, according to a new report by ThreatMetrix. While the cost of online orders lost to fraud is said to be around £2.92 billion, ThreatMetrix says that retailers could be losing out on an ever greater sum by employing fraud protection services that can’t identify genuine customers. According to the report, titled ‘Are You Treating Your Customers Like Criminals’, authentication protocols and password prompts which cause basket abandonment could be as much as ten times more costly than fraud.

**Technology**

- “The GitHub website, heavily frequented by coders and technical users, reported on Wednesday that it was operating normally for the first time in several days after attacks blamed on China.”
**Telecommunications**

- Sprint has agreed to a $131 million settlement of a class-action lawsuit accusing the company of defrauding investors about problems dating back to its $36 billion merger with Nextel Communications in 2005. Investors said the company falsely touted that the company was receiving billions of dollars of benefits from the merger and improving its subscriber base by tightening credit standards. Instead, investors said the company was struggling to integrate its cellular networks and was losing hundreds of thousands of subscribers, culminating in a $29.7 billion goodwill write down in February 2008.

**Defense**

- For the past two years, a cyberespionage group that likely operates from Lebanon has hacked into hundreds of defense contractors, telecommunications operators, media groups and educational organizations from at least 10 countries. The still-active attack campaign was uncovered and analyzed recently by security researchers from Check Point Software Technologies, who dubbed it Volatile Cedar. The company’s researchers found evidence that the attackers started their operation in late 2012, but have managed to fly under the radar until now by carefully adapting their tools to avoid being detected by antivirus programs. Unlike most cyberespionage groups, the Volatile Cedar attackers do not use spear phishing or drive-by downloads to gain a foothold into their victims’ networks. Instead they target Web servers and use them as initial entry points.

**Law Enforcement**

- Two former federal agents are accused of stealing bitcoins while investigating the online drug marketplace Silk Road. The Huffington Post reports that Carl Force, 46, a former DEA special agent, and Shaun Bridges, 32, an ex-special agent with the Secret Service, were arrested and charged, the Justice Department announced Monday. Force has been charged with wire fraud, money laundering, conflict of interest and theft of government money. Bridges faces charges of wire fraud and money laundering.

**Energy**

- Snohomish County (WA State) Train Watch is soliciting volunteers to identify, track and document train traffic passing through the county during the week of April 19-25. The group is specifically concerned about oil trains, and claims to be planning to hand the gathered data to local officials and emergency responders.

- Boston College’s student divestment campaign is organizing a Divestment March for April 12.

- A power surge in Stockton, CA led to a series of smart meter explosions. Local and international media are speculating as to why the smart meters were disproportionately affected by the surge, relative to analog meters.

**Agribusiness**

- Indiana legislators are currently considering two bills requiring the labeling of GMO’s. Activists are encouraging constituents to contact their representatives asking for support of HB 1460 and SB60.

- On March 30, CBS News published a story by Jessica Firger about the effects of pesticide consumption on sperm count. The story cites a recent study published in the
journal Human Reproduction, which measures subjects' sperm counts compared with the amount of pesticides consumed daily. Those consuming higher amounts of pesticides were found to have lower sperm counts.

- The Environmental Working Group (EWG) released a study this week which disagrees with the Big Ag and biotech companies’ repeated claims that GMO's will increase global food security. The report recognizes methods of improving food production by investing in infrastructure and basic resources for farmers in developing countries rather than developing genetically modified crops as a more effective method of increasing food security.

- The FBI says yes, and it has invoked the broader powers afforded by the Foreign Intelligence Surveillance Act, or FISA, to surreptitiously gather evidence against two Chinese siblings accused of plotting to steal patented seed from Iowa cornfields, according to court records. Stealing hybrid seeds enhanced with traits such as drought resistance doesn't pose the same immediate threat as a suicide bomber, but the FBI treats economic espionage and similar trade secret theft as dangerous threats to national security.

**Insurance/Healthcare**

- The de-identification of data is an important part of healthcare technology, especially as the use of EHRs and HIEs becomes more prominent. The HIPAA Privacy Rule states that once data has been de-identified, covered entities can use or disclose it without any limitation. The information is no longer considered PHI, and does not fall under the same regulations and restrictions as PHI.

- As more mega-breaches occur, cyber-insurers will more closely assess the security risks of potential clients, leading more organizations to improve their information security programs, attorney John Yanchunis predicts. "When companies are unable to get insurance ... you’re going to see companies adopting better security systems,” says Yanchunis of the Florida-based law firm Morgan & Morgan, who's representing consumers in several breach-related lawsuits. Those cases include one of the class action suits filed against Premera Blue Cross in the wake of a hacking incident that affected 11 million individuals.

- While EHRs and HIEs are being touted as necessary tools for the improvement of the nation’s healthcare system, some Californians believe that the use of HIEs in fact worsen patient data privacy, according to a recent study. Approximately 40 percent of respondents think HIE worsens privacy, while nearly one-third think it improves privacy and 42.5 percent believe it worsens security, according to a study published in the Journal of the American Medical Informatics Association. The study interviewed 800 adult California residents and conducted by University of California, Davis and University of California San Diego researchers.

- A new report by Atlantic Council think tank and Intel Security serves as a reminder about the importance of medical device cybersecurity. But it’s also a wake-up call for healthcare organizations to seriously consider consumer wearable health devices in their risk management strategies.

- Cloud security adoption is increasing in popularity, and the healthcare and pharmaceutical industries are leading the way, according to a recent CipherCloud survey. Those two industries represent 38 percent of respondents who are currently using cloud security services. The top four industries in terms of cloud adoption also include banking and finance, telecommunications, and government.

- We are just three months into 2015, and two large scale health data breaches have already taken place. The Anthem data breach affected approximately 78 million individuals, while Premera Blue Cross’ incident could impact nearly 11 million members and applicants. What do these two health data breaches have in common?
Not only are millions of individuals potentially affected, but each incident was caused by a cyber attack. Both Anthem and Premera reported that a third-party inappropriately broke into a database that contained individuals’ sensitive information – and in Premera’s case PHI as well.

- Five class action lawsuits have been filed in federal court against Premera Blue Cross in the wake of a data breach that affected 11 million individuals across the country. Meanwhile, its CEO has provided answers to questions from a U.S. senator regarding the hacker attack. The five lawsuits filed last week in the U.S. District Court in Seattle make similar allegations - that the company failed to protect customers’ confidential information, putting those affected at risk for identity theft. Among the complaints' allegations is that the data breach resulted from Premera's alleged "failures to follow HIPAA."

---

**Financial**

**Financial Services**

**Activism**

- LGBT activist groups will hold a protest outside a leading regional bank headquarters in Winston-Salem, NC on April 6 to speak out against Senate Bill 550 recently introduced by the North Carolina General Assembly. The groups compare SB550 to Indiana's SB 101 which is allegedly designed to allow businesses, organizations and individuals to discriminate against anyone in Indiana on religious grounds. This rally will be a part of a LGBT activist group’s national collaboration efforts of all actions against religious discrimination policies happening across the country.

- Activists held a 'Pack the Courtroom' rally outside the Richard J. Daley Center in Chicago, IL on April 2 to show support for a 75-year-old local resident as she fought an eviction case filed by her son.

- An anti-hedge fund activist group conducted an unannounced protest on Tuesday, March 31 in lower Manhattan to dispute Governor Cuomo's tax credit for luxury boats purchased over $230,000. The tax credit allows buyers to not pay sales tax beyond $230,000 on such boats.

- ‘Fight for $15’ rallies will occur on April 15 across the globe. Workers and labor activists will organize and conduct rallies demanding a $15 minimum wage and the right to form unions without retaliation. The ‘Fight for $15’ movement originated in New York City in 2012 and expanded to over 150 U.S. cities in 2014 with actions also occurring in 33 countries and six continents. New York City is expected to be the primary location for 2015 actions.

- The fifth annual Earth Day World Naked Bike Ride event will occur April 18 in San Francisco, CA in which participants plan to bicycle throughout the Financial District to bring awareness to environmental concerns.

**Information Security Risk**

- The Russian Ministry of Internal Affairs, together with the Federal Security Service, began taking steps to locate a cybergang targeting ATMs using the Tyupkin malware. The criminal operation consists of two stages. First, the gang gains physical access to the ATMs and inserts a bootable CD to install the malware. Following a successful infection, the malware runs in an infinite loop waiting for a command. To make it harder for the malware to be detected, Tyupkin only accepts commands at specific times on Sunday and Monday nights to take out the cash from the infected machines. When the combination key is entered correctly, the ATM displays details of how much cash is available in each cassette, inviting the operator to choose which cassette to rob. Soon the ATM dispenses 40 banknotes at a time from a chosen cassette. Tyupkin has been used to rob ATMs around the world, including several EU states, the US, and China.
Most attacks are made possible due to the widespread use of Microsoft's XP operating system in many ATMs. The malware is equipped with several features including skimming capabilities and an ability to read data from cards' magnetic strips and save PIN-codes.

- A British airline locked down thousands of frequent flyer accounts after a mass cyber-attack from an unknown source. The company announced that it froze the accounts after becoming aware that its systems had been hacked on a mass scale. The airline maintained that although the affected accounts number in the tens of thousands, no personal details of frequent flyers had been accessed or stolen.

- A pro-ISIS hacker group claimed to have compromised accounts at a federal credit union headquartered in Alexandria, Virginia.

- The Federal Financial Institutions Examination Council on Monday, March 30 issued two alerts, one concerning cyberattacks compromising credentials, and the other detailing destructive malware threats and related safeguards that the organization recommends. The FFIEC warned U.S. financial institutions that they're at increased risk from attacks that are designed to steal online credentials for the purpose of committing fraud or disrupting business as well as from destructive malware attacks that are designed to wipe all data from a system and "brick" devices, leaving them unbootable. The FFIEC recommends that the advisories be routed to every organization's CEO, CIO and CISO.

- A US online retailer specializing in mobile device accessories and safety products suffered a data breach that may have compromised the account details of about 50,000 customers. According to an official statement, on March 11, the company was notified by its website hosting company that it had been attacked, and that a relatively small number of credit card numbers were compromised and viewed by an outside party between March 3 and March 11, during order processing. The company also said they removed the malicious code that the hackers had inserted on their website and took steps to prevent any further unauthorized access to their data.

- An advanced RAT (Remote Administration Tool) known as DarkComet is targeting Danish businesses. The malware is delivered via email that's designed for spear-phishing. The payload, DarkComet, is stored in a Dropbox account and once downloaded and executed, it automatically begins collecting and stealing data from the compromised system. The threat includes features like keystroke capture, stealing data from the clipboard, taking screenshots, activating webcams and microphones, or setting up a remote desktop session.

- A new study found that a staggering 40% of companies estimate hourly losses of over £100,000 at peak times during a DDoS outage, a 470% rise compared to last year. The study shows that multiple attacks are also becoming more prevalent and are lasting even longer than those recorded in the last survey, with more than a third of attacks affecting businesses for more than 24 hours. Additionally, 52% of companies attacked find themselves the victims of theft, with 24% more businesses reporting loss of customer data, intellectual property or money during a DDoS attack compared to last year.

- Researchers identified a 64-bit version of NewPosThings, a point-of-sale (PoS) malware designed to steal payment card and other sensitive information from infected systems. The malware, detected as TSPY_POSNEWT.SM, installs itself on a device using names such as javaj.exe, ism.exe, svchost.exe, dwm.exe and isasss.exe. Once installed, NewPosThings starts collecting passwords for virtual network computing (VNC) software such as UltraVNC, RealVNC, WinVNC, and TightVNC. Then, the Trojan disables the operating system's security warnings for certain file extensions, including .exe, .bat, .reg and .vbs.

**Legal, Litigation, Regulatory Risk**

- An appeals court rejected a suit by investors who argued that the Securities and Exchange Commission was negligent in not spotting the Allen Stanford Ponzi scheme. Stanford was sentenced to 110 years in prison for fleecing investors who thought he
was putting their money into high-interest CDs. In a ruling issued last week, an appellate court agreed with a lower court’s decision that the SEC enjoys sovereign immunity and owes investors nothing.

- The White House is backing a proposed rule that would require brokers handling retirement accounts to put the interest of their clients ahead of their own, a so-called fiduciary standard long required of lawyers, doctors and some financial professionals like registered investment advisers. In announcing its support for stricter standards, the White House cited a report from its Council of Economic Advisers that estimates that brokers with conflicts of interest are cutting returns in individual retirement accounts by 1 percent a year, or about $17 billion. The article added that details of the proposed rule haven’t been hammered out, but lobbying for and against it is already intense.

- President Barack Obama signed an Executive Order on Wednesday, April 1 allowing the use of economic sanctions for the first time against perpetrators of destructive cyber-attacks and online corporate espionage. The move will let the Treasury Department freeze the assets of overseas individuals and entities identified as the source of cybercrimes. The federal government also will be able to bar U.S. citizens and companies from doing business with those targeted for sanctions.

**Operational Risk**

- Czech police seized a luxury property purchased with Bitcoin by a couple previously linked to the hack of an underground drug market set up as a Tor hidden service. The infamous online drug market shut down in December 2013, following claims that hackers had absconded with approximately $5.3m in Bitcoin. Users who tracked the stolen funds on the blockchain (a public ledger of all Bitcoin transactions) voiced suspicions that the theft was an inside job.

**Reputational Risk**

- Customers of a leading Swiss bank in India suspected of tax evasion were given 30 days to nominate a legal representative in Switzerland or face seeing their names published in the country’s official gazette. The bank has in the last two weeks forwarded a letter from the Swiss government to a select number of Indian customers, which warns that Switzerland is now prepared to give “administrative assistance” to Indian tax investigators. Customers have one month to nominate a third party based in Switzerland, such as a lawyer, to manage or challenge the disclosure process on their behalf.

---

**Global Intelligence**

**China**

- A forum post on Bitcointalk.org reports a Chinese bitcoin trading network, BtcTrade, suffered multiple DDoS attacks since March 26. According to the post, the attacks stopped on March 30th but the network has not returned to normal yet.

- An article on 51cto.com reports that the Chinese super computer Tianhe 1 contains multiple security vulnerabilities. According to the article, the Tianhe network contains more than 500 users and 200 of those users have weak passwords. In addition, the Shellshock vulnerabilities in the system still have not been patched.

- An article on II168.com reports that a malicious Trojan named “Black Fox” has infected nearly one million users. According to the article “Black Fox” can be controlled remotely, and it promotes malware and avoids detection by most mainstream anti-virus applications, and is sometimes disguised as a legitimate application.

- A posting on Btcfans.com reports that after BtcTrade experienced several waves of DDoS attacks, another Chinese bitcoin trading platform, Bitbays is now being targeted. Currently, the official website of Bitbays is still not able to display properly.
A posting on Jb51.net, a Chinese script repository, reports that they have suffered two DDoS attacks recently and they are currently collaborating with the police to locate the attackers.

**North America**

- DSL Reports reported that with the FCC recently ruling that ISPs are common carriers under Title II; the agency is beginning to explore whether it should use its newly-established authority to impose new consumer protections. This week, the FCC announced that it will be holding a privacy roundtable on April 28 to begin examining a “harmonized privacy framework” across various telecom services. The FCC notes it decided to forbear from requiring broadband companies to adhere to rules requiring phone companies protect customer proprietary network information (CPNI) and wants to examine rules better suited for broadband and wireless networks.

- DSL Reports reported that last month Verizon decided not to pay the fee increases demanded by The Weather Channel and so the channel has been pulled from the FiOS TV lineup. In an effort to generate some consumer outrage The Weather Channel initially launched a new campaign urging FiOS customers to reach out and complain to Verizon. With that not working very well, The channel has launched a new series of ads mocking competitor AccuWeather for not covering enough weather. According to the article, most of the comments from FiOS users, who’ve been without the channel for nearly a month, indicate most people aren’t going to miss the channel.

- DSL Reports reported that the Radio Shack brand has won a last minute reprieve from a U.S. bankruptcy court to remain in business. It will be operating around 1,700 stores cooperatively with Sprint. The deal not only keeps the Radio Shack brand from heading the way of the Betamax and Laser Disc, it will help keep roughly 7,500 jobs intact. The deal will also more immediately double the retail presence for Sprint, which will occupy a third of each store. The deal also (for now) eliminates concerns that a flood of personal user information was among the properties being auctioned off to the highest bidder.

**Legal and Regulations**

- On March 23, the Federal Trade Commission ("FTC") Bureau of Consumer Protection ("Bureau") announced the formation of the Office of Technology Research and Investigation ("OTRI"), a branch that will expand the agency’s technological capabilities by identifying ways to continue to protect consumers during a time of rapid technical innovation. The Bureau’s blog post regarding OTRI is available [here](#).

- In an attempt to verify compliance with the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule, the Office of Civil Rights (OCR) for the United States Department of Health and Human Services piloted privacy and security audits of covered entities in 2011 and 2012 (the “Phase 1 Audits”). Phase 2 Audits will likely begin soon. In the meantime, covered entities and business entities should take advantage of the delay by reviewing their current HIPAA compliance programs.

- On March 25, the House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade took action that brings us closer to federal data security and data breach legislation—the Data Security and Breach Notification Act of 2015 (DSBN). The DSBN is intended to create a single national security and breach notification standard for most private sector organizations that handle personal information in electronic form, including telecommunications common carriers, nonprofits and companies ordinarily subject to the Federal Trade Commission’s (FTC) jurisdiction (collectively, “covered entities”). The bill requires covered entities to “implement and maintain reasonable” security measures to protect personal information and establishes breach notification obligations for covered entities that suffer a data security breach. The current version of the bill would require covered entities to notify affected individuals within 30 days of taking the steps necessary to
investigate the breach and restore the “integrity, security and confidentiality” of affected systems. If a covered entity reasonably suspected that a breach affected more than 10,000 individuals, the covered entity would be required to notify the FTC, the Secret Service or the Federal Bureau of Investigation “as expeditiously as possible.”

- The Judicial Conference Committee recently approved changes to Federal Rule of Civil Procedure 37(e) addressing preservation and sanctions and setting forth clearer and more reasonable preservation standards than those imposed by some courts in the past. See Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure, Agenda E-19 (Sept. 2014). The proposed change awaits review by the United States Supreme Court and, if approved, will take effect on December 1, 2015 (absent action by Congress). The new language of Rule 37(e) applies only to electronically stored information (ESI).

- Two recent decisions, one from the Delaware Court of Chancery and one from the California Court of Appeal, Fourth Appellate District, refused to apply bylaws that impaired a shareholder/member plaintiff’s ability to pursue his or her claims against the corporation where the the relevant bylaw was adopted after the plaintiff’s claims accrued. Strougo v. Hollander, C.A. No. 9770-CB, 2015 WL 1189610 (Del. Ch. Mar. 16, 2015). Cobb v. Ironwood Country Club, 233 Cal. App. 4th 960 (2015).

- On March 24, the U.S. Supreme Court heightened the importance of U.S. Trademark Trial and Appeal Board (“TTAB”) decisions in related trademark infringement litigation which will likely result in brand owners having to battle more extensively in TTAB actions. B&B Hardware, Inc. v. Hargis Industries, Inc., ___ U.S. ___ (2015). The Court held that a prior TTAB ruling on likelihood of confusion between two trademarks can, in certain circumstances, be binding in a related trademark infringement action in federal court. This is a significant ruling because TTAB administrative proceedings determine whether or not a trademark is capable of registration, not use. Under B&B Hardware, TTAB rulings now have the potential to impact use of a trademark, which has significant implications for brand owners’ U.S. registrations and enforcement strategies and will require that TTAB actions be taken all the more seriously.

- Following President Obama’s December 2014 announcement of a relaxed policy towards Cuba, many companies await the opening up of the Cuban market. Some steps can be taken now to protect a company’s valuable trademarks and other IP in Cuba. An exception to the long-standing US embargo on trade with Cuba permits US companies to file for and obtain trademark registrations in Cuba. US companies should consider taking immediate action to protect their trademark rights in that country. Doing so is advisable because Cuba is a “first to file” jurisdiction – in other words, a Cuban registration for a trademark will be awarded to the first applicant, even if that applicant has no legitimate claim to the mark.

- Three of the most popular social media platforms—Facebook, Twitter and Reddit—have recently amended their terms of use to state that they will remove digital images of nudes that have been posted without the subjects’ permission. “Twitter executives have said the company will lock the accounts of users who post content that violates their user policy,” Mashable reports. These policies are critical weapon in the war against revenge porn because they can be used to remove revenge porn photos before they have been widely disseminated.

Canada

- This month marks the issuance of the first two enforcement actions under Canada’s Anti-Spam Law (CASL) since provisions governing commercial electronic messages (CEMs), software downloads, and related conduct took effect July 1, 2014. CRTC imposed over US$900,000 in fines against two companies, reminding U.S.- and foreign-based businesses about possible liability under Canada’s Anti-Spam Law. On March 5, the Canadian Radio-Television and Telecommunications Commission (CRTC) announced that it had imposed a fine against Compu.finder Inc., claiming the company violated CASL by sending CEMs to individuals without the recipients’ consent. On March 25, the CRTC announced a settlement with Plentyoffish Media, Inc. While the CRTC thus far has cited only two domestic companies, all companies
wherever located doing business in Canada should take note, especially as CASL’s final provisions go into effect over the coming two years. 

- The ‘notice and notice’ provisions of Canada’s Copyright Modernisation Act have now come into force (SC 2012, c 20 Section 47 was brought into force by Statutory Instrument 2014-58). The provisions allow a copyright owner to provide an internet service provider (ISP) with a notice of alleged copyright infringement and to require the ISP to forward it to the subscriber. They also require the ISP to maintain its records relating to the subscriber for a certain period so that the rights holder may seek to obtain the information for the purpose of litigation.

**Pharmaceuticals**

- As it beefs up its vaccines business, Pfizer’s looking to bolster revenue from the top-selling Prevenar family of shots. But on that front, it’s come up against a roadblock in China—and so it’s shutting down its vaccines marketing there.

- A campaign to reduce the use of animals for medical research in the U.K. is causing howls of protest from scientists who say such a move would effectively ban nearly 89% of research that is conducted. The campaign was started recently by the British Union for the Abolition of Vivisection. The advocacy group, which wants to end all animal experiments, asked members of the U.K. parliament, as well as candidates running for seats in the governing body in upcoming May 7 election, to sign a six-point pledge to curtail the use of animal in medical research.

- More researchers are leaving multinational drug makers for Chinese startups, reflecting a growing optimism in the pharmaceutical industry based in China.

- One day after Valeant Pharmaceuticals closed its acquisition of Salix Pharmaceuticals, the acquisitive drug maker disclosed it would lay off 258 workers in North Carolina.

**Retail**

- Online retailers battling with fraud prevention are losing out on genuine sales by treating their customers like criminals, according to a new report by ThreatMetrix. While the cost of online orders lost to fraud is said to be around £2.92 billion, ThreatMetrix says that retailers could be losing out on an ever greater sum by employing fraud protection services that can’t identify genuine customers. According to the report, titled ‘Are You Treating Your Customers Like Criminals’, authentication protocols and password prompts which cause basket abandonment could be as much as ten times more costly than fraud.

- While businesses across the state of Indiana voice concern over the impact of the Religious Freedom Restoration Act, local shop owners are losing customers both in and out of state.

- The Globe and Mail reported that late on April 1, the Commodity Futures Trading Commission in the United States accused Kraft Foods Group Inc. and its former parent, Mondelez International Inc., of manipulating wheat prices a few years ago. The CFTC sued the two companies in federal court, alleging this was done via purchases of some $90-million (U.S.) of futures. No allegations have been proven in court.

- Forbes reported that home improvement retailer, Lowe’s, is experimenting with an in-store robot that would help customers find what they need when they enter a Lowe’s location. According to Engadget, each robot is equipped with a touchscreen as well as a voice recognition module that a customer can use to input a command. Lowe’s is right there with some of the other industry giants who are incorporating e-commerce
and tech-enabled stores to create a true omnichannel experience. For investors, this presents an intriguing opportunity to get an early jump on an under-publicized growth opportunity.

- Gizmodo reported that back in February, RadioShack filed for Chapter 11 bankruptcy, destroying the childhood memories of many a tech blogger, and putting 4,000 brick-and-mortar stores in jeopardy at the same time. But as of today, a plan to co-brand remaining stores with the Sprint logo is officially approved. As reported by Reuters, the offer to co-brand 1,740 remaining RadioShack stores as Sprint/RadioShack locations received approval in bankruptcy court today. Stores will apparently carry both names, with Sprint occupying about a third of each location.

- The Bookseller reported that a US campus retailing group has filed a lawsuit against Purdue University in Indiana, claiming that it is withholding public information about its contract with Amazon. The university worked with Amazon to launch the Purdue Student Store last August.

- The Star reported that Target Corp. is planning to close all of its Canadian stores even faster than originally planned. A court-appointed monitor overseeing the windup of the Target Canada stores says all 133 locations across the country will be permanently shut down by “as early as mid-April,” which is about a month ahead of schedule.

- eMarketer reported that according to research from TechnologyAdvice in March 2015, 60% of US adult internet users read marketing emails, however, just 16% do so regularly, and only 12.8% read more than half of the ones they received. Taking a quality over quantity approach is key for email marketers looking to outshine the inbox competition. When asked how businesses could improve their email efforts, nearly 44% of internet users said sending less emails would help. Meanwhile, nearly half wanted more informative content or personalized offers.

- USA Today reported that McDonald’s rivals could be forced to match the raises that the chain is handing out as they compete harder for fast-food and retail workers. McDonald’s said it plans to increase pay at least $1 more than the local minimum wage on July 1 for the 90,000 employees at corporate-owned restaurants. It expects wages to rise to more than $10 an hour by the end of 2016. The hike, more than 10%, follows similar announcements in recent months by Walmart, Target and TJX Stores and protests by low-paid workers nationwide the past two years calling for base wages of $15.

- The authors of NewPoSThings malware that targets payment processing systems have launched new releases in the wild, aiming at infecting 64-bit machines with increased version numbers. Currently at version 3.0, security researchers say that the most recently spotted samples of the point-of-sale (PoS) malware may have been compiled during the last week of January.

Technology

- The new malicious software called the Laziok Reconnaissance trojan designed to steal information on the infected system to provide useful details that would allow the threat actors to decide on the best course of action. The malware targets the energy sector with the focus on the Middle East. The campaign has been observed running between January and February.

- IBM Security has identified an active campaign using a variant of Dyre malware that has successfully stolen more than $1 million from targeted enterprise organizations. The campaign, named “The Dyre Wolf” by IBM Security researchers, shows a brazen twist from the once-simple Dyre malware by adding sophisticated social engineering tactics likely to circumvent two-factor authentication.

- The European Union is weighing a major investigation into how Internet platforms like Google Inc. and Amazon.com Inc. operate in Europe, amid concerns that such
companies have too much power over smaller firms.

- “The GitHub website, heavily frequented by coders and technical users, reported on Wednesday that it was operating normally for the first time in several days after attacks blamed on China.”

---

**Telecommunications**

- Sprint has agreed to a $131 million settlement of a class-action lawsuit accusing the company of defrauding investors about problems dating back to its $36 billion merger with Nextel Communications in 2005. Investors said the company falsely touted that the company was receiving billions of dollars of benefits from the merger and improving its subscriber base by tightening credit standards. Instead, investors said the company was struggling to integrate its cellular networks and was losing hundreds of thousands of subscribers, culminating in a $29.7 billion goodwill write down in February 2008.

- DSL Reports reported that months after Verizon promised that they let users opt out of both the specialized ads and the covert traffic manipulation, Verizon has announced that user can actually do so. Customers can opt out by visiting Verizon's privacy settings website, or by calling 866-211-0874.

---

**Defense**

- For the past two years, a cyberespionage group that likely operates from Lebanon has hacked into hundreds of defense contractors, telecommunications operators, media groups and educational organizations from at least 10 countries. The still-active attack campaign was uncovered and analyzed recently by security researchers from Check Point Software Technologies, who dubbed it Volatile Cedar. The company’s researchers found evidence that the attackers started their operation in late 2012, but have managed to fly under the radar until now by carefully adapting their tools to avoid being detected by antivirus programs. Unlike most cyberespionage groups, the Volatile Cedar attackers do not use spear phishing or drive-by downloads to gain a foothold into their victims’ networks. Instead they target Web servers and use them as initial entry points.

- The U.S government’s Defence Advanced Research Projects Agency (DARPA) has prioritized the development of a more dependable and efficient real-time location tracking technology due to the incompetence of GPS in specific situations. The United States Department of Defense, has been involved in developing “radically” new technological solutions to offer an advanced and efficient position-and-navigation tracking mechanism. It aims at developing a more trustable and accurate system than the currently available Global positioning System (GPS).

- President Barack Obama launched a sanctions program on Wednesday to target individuals and groups outside the United States that use cyber-attacks to threaten U.S. foreign policy, national security or economic stability.

- U.S. intelligence officials say China has dramatically increased spending on the development of more advanced cyber capabilities in an effort to level the playing field where offensive capabilities are concerned. In March, the Chinese military formally acknowledged the nation has multiple units in place specifically tasked with cyber warfare and intelligence operations.
Law Enforcement

- The FBI said it does not believe an attack at the guarded gates of the NSA last week was terrorism. The bureau launched an investigation after two men who were allegedly dressed as women disobeyed commands at the gates of the NSA in Fort Meade, Md., crashing a stolen car into a police vehicle. One of the men died, and the other was injured from gunshots.

- Two former federal agents are accused of stealing bitcoins while investigating the online drug marketplace Silk Road. The Huffington Post reports that Carl Force, 46, a former DEA special agent, and Shaun Bridges, 32, an ex-special agent with the Secret Service, were arrested and charged, the Justice Department announced Monday. Force has been charged with wire fraud, money laundering, conflict of interest and theft of government money. Bridges faces charges of wire fraud and money laundering.

- FBI Director James Comey is lobbying Congress to create a law that would require tech companies to "create a backdoor into any communications device that uses encryption," Gizmodo reports.

- Two St. Louis men accused of planning bomb attacks during protests in Ferguson have been indicted on federal charges, the U.S. Attorney's office in St. Louis said Thursday. Olajuwon Davis and Brandon Orlando Baldwin, both 22, are facing several charges, including conspiracy to use explosives and making false written statements while buying firearms. The indictment alleges the men conspired from September through November 21 to obtain explosives, and Davis paid a deposit before both were arrested when they arrived at a location where they thought they'd be picking up the explosives. The indictment alleged the men were affiliated with the local chapter of the New Black Panther Party.

- Families of the hostages of a radical gunman who killed four in a kosher supermarket are suing a French broadcaster over its live coverage of the attack, saying it endangered the hostages' lives. Paris prosecutor's office spokeswoman Agnes Thibault-Lecuivre said Friday that a preliminary investigation has been opened into the coverage by BFM all-news television, on possible charges of "putting others' lives in danger." France's broadcast watchdog reprimanded BFM and several other television and radio stations for their coverage of the market hostage-taking and attack on satirical newspaper Charlie Hebdo in January. BFM and other broadcasters notably revealed in live reports that shoppers were hiding in the kosher market. The watchdog and the families' lawyers say that could have endangered the hostages if the gunman found out.

- Two women living in Queens have been charged with planning to build a bomb, in a plot revealed by a monthslong undercover investigation that found the women had discussed the merits of various types of bombs and had obtained four propane gas tanks. The women, Noelle Velentzas, 28, and Asia Siddiqui, 31, who until recently were roommates in Queens, were named in a complaint unsealed on Thursday in Federal District Court in Brooklyn, where they appeared Thursday afternoon. Ms. Velentzas and Ms. Siddiqui, who are American citizens, talked about jihad as they studied bombs. Ms. Siddiqui had been communicating with Al Qaeda in the Arabian Peninsula, and Ms. Velentzas had watched violent videos made by the Islamic State, also known as ISIS, the complaint says. In the complaint, the government said the plot advanced to the point that Ms. Siddiqui bought four propane gas tanks and stored them in a stairwell outside her apartment. Earlier, the women had shopped for potassium gluconate at a Queens pharmacy, bought Miracle-Gro fertilizer, which can be used as a bomb component, and read about and discussed making bombs like the pressure-cooker bombs used in the Boston Marathon attack.

- Four journalists arrested during last summer's Ferguson protests over the shooting death of Michael Brown filed a federal lawsuit Monday against St. Louis County police and 20 of its officers, accusing them of violating the reporters' civil rights and
unjustifiably detaining them. The lawsuit, filed Monday in St. Louis, alleges the arrests
for the journalists' failure to disperse as demanded by police on August 18 and August 19
were "undertaken with the intention of obstructing, chilling, deterring, and retaliating
against (the) plaintiffs for engaging in constitutionally protected speech, newsgathering
and recording of police activities."

- The messaging app Snapchat released its first ever transparency report last week,
bringing the company in line with common practices used by Google, Facebook and
other large technology companies. From November 1, 2014, until February 28, 2015,
Snapchat said it received 375 requests from law enforcement for information in the
United States. The company reported complying with 92 percent of those queries.