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

Cyber Safety Awareness Training

Protect your Organization with Computer-Based Training

Are your employees the weak link in your security program? We want to help you educate your employees to keep them — and your organization — more secure.

Our computer-based cyber security training can help your employees learn how to protect your organization from the latest threats and reduce the high costs associated with incident remediation.

Top Incidents

Energy

- February 13, 2015 has been dubbed “Global Divestment Day.” Protests are promised around the world in order to urge endowments and public pensions to end their investments in carbon-based energy.

Agribusiness

- Farmers and peasants say they have not offered to sell their land to make way for the new canal, which the Nicaraguan government says will solve the country’s economic problems. Scores of Nicaraguan protesters have been arrested and dozens injured as
Nicaraguan police broke up road blocks set up by demonstrators protesting this week against possible eviction from their lands due to the construction of an interoceanic canal in the country. Farmers and peasants say they have not offered to sell their land to make way for the new canal, which the Nicaraguan government says will solve the country’s economic problems.

**Insurance/Healthcare**

- The five biggest 2014 health data breaches listed on the federal tally so far demonstrate that security incidents are stemming from a variety of causes, from hacker attacks to missteps by business associates. The top breaches offer important lessons that go beyond the usual message about the importance of encrypting laptops and other computing devices to prevent breaches involving lost or stolen devices, still the most common cause of incidents. They also highlight the need to bolster protection of networks and to carefully monitor the security practices of business associates.

**Financial Services**

- North Korea threatened unspecified attacks on the US in an escalation of a war of words following the cyber-attacks on a Japanese American motion picture company. The North warned of strikes against the White House, Pentagon and "the whole US mainland." North Korea denies US claims it is behind cyber-attacks linked to a film that features the fictional killing of its leader Kim Jong-un.

**Global Intelligence**

- The German Chaos Computer Club, Europe's largest hacker association, organized its 31st convention for December 27-28, 2014, with 120 presentations and dozens of workshops under the title, “A New Dawn,” or 31C3. Organizers hoped for 10,000 attendees. Important presentations related to hacks of biometric security features, vulnerabilities of mobile phone protocol SS7 or payment cards with implemented chips, as well as Internet surveillance programs. Additionally, a list of possible targets of NATO operation ISAF in Afghanistan was published during the convention in collaboration with German news magazine Der Spiegel.

**Legal and Regulations**

- On December 22, 2014, the Federal Trade Commission announced that it notified China-based BabyBus (Fujian) Network Technology Co., Ltd., (“BabyBus”) that several of the company’s mobile applications (“apps”) appear to be in violation of the Children's Online Privacy Protection Rule (the “COPPA Rule”). In a letter dated December 17, 2014, the FTC warned BabyBus of potential COPPA violations stemming from allegations that the company has failed to obtain verifiable parental consent prior to its apps collecting and disclosing the precise geolocation information of users under the age of 13.

**Pharmaceuticals**

- China has agreed to streamline its regulatory processes and cut red tape for imports of new drugs, a move that should benefit the U.S. pharmaceutical industry, the U.S. Commerce Department says.

**Retail**

- Researchers with EMC's RSA Security Division have pulled back the covers from the Backoff malware in a new report. The Backoff malware made a big splash in the world of cybercrime in 2014, emerging as one of the most notorious pieces of point-of-sale malware in the wild. In August, the U.S. Secret Service linked it to compromises at 1,000 U.S. businesses. It was also linked to attacks on Diary Queen and the United Parcel Service (UPS). The report offers details of the malware's command and control infrastructure and how it operates. But perhaps more notably, it offers some indication the attacker or attackers controlling the malware may be in India.
Technology

- Facebook Inc., Twitter Inc. and Google Inc. have started resisting Russian government orders to remove information about a rally next month in support of opposition leader Alexei Navalny, raising the prospect of a showdown over the Kremlin’s efforts to control online information. In response to a request from Russian prosecutors, Roskomnadzor, the country’s communications regulator, began issuing block orders for Russia just hours after the Moscow rally was publicized on social media late last week, officials said. Facebook honored the initial order last weekend and blocked a page promoting the event, but others were quickly created, attracting more attention.

Telecommunications

- Republican Congressional leaders are proposing a new plan that could prevent service providers from giving priority for some websites over others, reports The Washington Post, citing unnamed industry officials close to the plans.

Defense

- Japan, South Korea, and the United States signed an agreement on 29 December to share classified information on North Korea’s nuclear and missile programs. Under the agreement, South Korea and Japan will pass information to the US Department of Defense, which will then classify it under existing bilateral agreements and share with the other country.

Law Enforcement

- Google alerted authorities to a Colorado Springs man who threatened to “hunt” and kill police officers in the comment sections of a YouTube video, leading to the man’s arrest. Jeremiah M. Perez was arrested after Google contacted the FBI Office in San Francisco. Mr. Perez’s threat read, “SINCE DARREN WILSON our group has killed 6 retired sheriffs and cops……because of this event we will hunt two more in colorado this week…..for every innocent citizen that cops kill WE, VETERANS WILL KILL RETIRED HELPLESS COPS,” the threat read. “COPS ARE THE REAL ENEMIES OF FREEDOM LOVING AMERICANS and TIME TO STRIKE BACK IN ALL OUT WAR IS NOW.” The user name of the commenter was “Vets Hunting Cops.”

Energy

- The Sierra Club has dubbed the EPA’s new coal ash standards a “modest first step” and has vowed to “use every tool available to strengthen this safeguard.” Since January 2013, the Sierra Club has openly used direct action protests as one of its available tools to press for legal and/or regulatory change.

- February 13, 2015 has been dubbed “Global Divestment Day.” Protests are promised around the world in order to urge endowments and public pensions to end their investments in carbon-based energy.

- Activists in the United States and Canada have begun using infrared video to record and track emissions at fracking sites. This coincides with increased attention by local community groups on monitoring refinery emissions through private sensor networks.

- By the end of 2015, Pope Francis is expected to tell the planet’s 1.2 billion Catholics why acting on climate change is essential to the faith using an influential church document called an encyclical. This has been long-rumored, but will reportedly be released to the world’s 5,000 bishops and 400,000 priests following a papal visit to the hurricane-damaged city of Tacloban in the Philippines.
Agribusiness

- Farmers and peasants say they have not offered to sell their land to make way for the new canal, which the Nicaraguan government says will solve the country’s economic problems. Scores of Nicaraguan protesters have been arrested and dozens injured as Nicaraguan police broke up road blocks set up by demonstrators protesting this week against possible eviction from their lands due to the construction of an interoceanic canal in the country. Farmers and peasants say they have not offered to sell their land to make way for the new canal, which the Nicaraguan government says will solve the country’s economic problems.

- California’s new humane-treatment rule for egg-laying hens takes effect on January 1, 2015 and is having an impact on producers as far away as Pennsylvania, says Bloomberg. The California rule requires farmers to give hens enough space to stand, extend their wings and lie down if they want to sell eggs in the state.

- Chinese lawmakers are considering a proposed law to require labeling of all foods that contain genetically modified organisms.

- Farmers already scrambling to find workers in California — the leading U.S. grower of fruits, vegetables and nuts — fear an even greater labor shortage under President Barack Obama’s executive action to block some 5 million people from deportation. Thousands of the state’s farmworkers, who make up a significant portion of those who will benefit, may choose to leave the uncertainty of their seasonal jobs for steady, year-around work building homes, cooking in restaurants and cleaning hotel rooms.

Insurance/Healthcare

- Two essential elements of medical practice—patient privacy and the patient-physician relationship—are at stake in a case before a federal appeals court that involves a state prescription drug monitoring program (PDMP) and surveillance by the U.S. Drug Enforcement Administration (DEA).

- Sony Pictures Entertainment could be penalized by regulators for the data breach that resulted in private health information of its employees becoming public, and could be socked with lawsuits as well. It remains to be seen which regulators might target the company, or which rules it might be accused of violating, but, regardless of who wields the hammer, there are lessons other companies can learn from this to better protect the health information of their workers.

- The five biggest 2014 health data breaches listed on the federal tally so far demonstrate that security incidents are stemming from a variety of causes, from hacker attacks to missteps by business associates. The top breaches offer important lessons that go beyond the usual message about the importance of encrypting laptops and other computing devices to prevent breaches involving lost or stolen devices, still the most common cause of incidents. They also highlight the need to bolster protection of networks and to carefully monitor the security practices of business associates.
Financial Services

Activism

- Activists are planning a series of actions to "end Corporate Personhood" to occur January 21, 2015 on Wall Street in New York City. The actions are meant to denounce the five year anniversary of the landmark ruling and official sanction by the Supreme Court.

- Activists held protests at Federal Reserve Banks on December 23, 2014, the 100th birthday of the Federal Reserve.

Information Security Risk

- Researchers based in the Netherlands and Russia claimed that the reason U.S. retailers were plagued by so many breaches in 2014 is because a ring of sophisticated financial cybercriminals in Russia and Ukraine have been targeting U.S. merchants and payments processors with malware. The ring, known as Anunak, which includes the hackers who developed Carberp, a banking Trojan that emerged in 2010, has reportedly tweaked its techniques and broadened its range of targets. While Anunak attacked 16 U.S. retailers in 2014, it also targeted a range of other businesses, including 50 banks in Russia and a handful of news media and public relations firms in various parts of the world.

- The largest U.S. office-supply retailer said 1.16 million payment cards may have been affected in a series of data breaches that occurred from July into September. The theft occurred after criminals deployed malware on point-of-sale systems at 115 of Staples' 1,400 U.S. stores. The company disclosed in October that it was investigating a potential breach.

- North Korea threatened unspecified attacks on the US in an escalation of a war of words following the cyber-attacks on a Japanese American motion picture company. The North warned of strikes against the White House, Pentagon and "the whole US mainland." North Korea denies US claims it is behind cyber-attacks linked to a film that features the fictional killing of its leader Kim Jong-un.

- Citing allegations that there is a renewed attempt to attack the Tor network, a known cyber threat actor group is calling on allies to save Tor by attacking every U.S. bank and government site.

- An article reported that the hackers that stole millions of depositors' contact information from the largest U.S. bank earlier this past summer didn't use any kind of sophisticated malware but managed to pull off the hack because the bank failed to upgrade one of its servers with two-factor authentication.

- A December 23, 2014 post to a prominent paste site references numerous websites of financial institutions that may be potentially targeted by the Dridex malware. Dridex is being touted as the successor of the banking malware Cridex, and aims at stealing personal information, specifically related data to online banking.

Legal, Litigation, Regulatory Risk

- U.S. Attorney for the Western District of Pennsylvania and U.S. Secret Service Special Agent in Charge of the Pittsburgh Field Office announced on December 18, 2014 the filing of a criminal complaint in Pittsburgh charging a U.S. citizen with leading an international counterfeit currency operation headquartered in the Republic of Uganda. The accused U.S. citizen, who currently resides in Kampala, Uganda, was charged with conspiracy and counterfeiting acts committed outside of the U.S. When he lived in the U.S., he mainly resided in Texas and Colorado.

- A U.S. regulator has denied a Russian oil firm's offer to purchase a leading U.S. investment bank's oil trading business. The deal was valued by sources at between
Operational Risk

- In reference to the numerous police brutality actions occurring across the U.S., multiple activist groups have threatened a physical ‘Winter of Resistance’ targeting politicians and “corporate kings.”

Reputational Risk

- A former executive who blew the whistle on a leading mortgage lender is expected to be paid $57 million for helping U.S. government collect a record $16.6 billion penalty for the lender’s role in the financial crisis.

- A Twitter rant on December 22, 2014 criticized a leading U.S. investment bank for continuing to do business with “Russians.”

Global Intelligence

Germany

- The German Chaos Computer Club, Europe’s largest hacker association, organized its 31st convention for December 27-28, 2014, with 120 presentations and dozens of workshops under the title, “A New Dawn,” or 31C3.. Organizers hoped for 10,000 attendees. Important presentations related to hacks of biometric security features, vulnerabilities of mobile phone protocol SS7 or payment cards with implemented chips, as well as Internet surveillance programs. Additionally, a list of possible targets of NATO operation ISAF in Afghanistan was published during the convention in collaboration with German news magazine Der Spiegel.

- FMag reported that Amazon staff at three German warehouses will extend their strike until Christmas Eve to increase pressure on the online retailer in a long-running dispute over pay and conditions. Verdi also filed a lawsuit against a decision by regional authorities to allow Amazon staff in two German cities to work this Sunday as the mail-order group steps up efforts to deliver order to customers before the Christmas holiday. Industrial action this week had already been extended until Saturday in four of Amazon’s nine distribution centers in Germany and until December 24, 2014 at one warehouse. More than 2,400 workers took part in walkouts on Friday, Verdi said.

India

- BGR reported that as Foxconn prepares to suspend operations at its facilities in in India, employee unions have threatened to launch a protest if the company stops production from December 23, 2014. Foxconn India Employees Union President stated that, “We will go to the plant everyday even if they ask us to go home. If they ask us to leave, we will not hesitate to go for protest.”

Israel

- Arutz Sheva reported that Prime Minister Netanyahu, acting Finance Minister, stated on December 21, 2014 that implementation to raise minimum wage to NIS 5,000 will begin in January.

North America

- The Family and Medical Leave Act requires employers to provide job-protected leave to eligible employees. Sometimes, employers receive FMLA requests from employees that involve shifts to the working schedule or other measures such as the ability to work from home. According to a new decision from the Seventh Circuit Court of
Legal and Regulations

- On December 18, 2014, President Obama signed five cybersecurity-related bills into law, an attempt to increase cyber protection in the wake of recent data breaches.
  - The first bill is the **Federal Information Security Modernization Act**, which eliminates the 12-year-old security review process that requires agencies to submit a checklist showing their IT processes comply with security standards and controls. Now, agencies are required to continuously monitor their systems. Additionally, the law codifies the practice of having the Office of Management and Budget determine IT security policies for federal agencies.
  - The second is the **Homeland Security Workforce Assessment Act**, a rider on the Border Patrol Agent Pay Reform Act, which more efficiently identifies and fills cybersecurity positions at the Department of Homeland Security (DHS). One provision of this law provides more competitive compensation to cybersecurity professionals. This law addresses the previous “slow and cumbersome hiring procedures” which have challenged DHS from competing for scarce cybersecurity talent in the past.
  - Third is the **Cybersecurity Workforce Assessment Act**, which requires DHS to adopt new strategies to enhance recruitment, training, and retention of its cybersecurity workforce.
  - Fourth is the **National Cybersecurity Protection Act**, which codifies the department's national cybersecurity center, the National Cybersecurity and Communications Integration Center. The center will be open continuously and serve as a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement. The center will facilitate the sharing of information to provide better understanding of cybersecurity risks, incidents, and recovery actions.
  - Finally, the **Cybersecurity Enhancement Act** authorizes the Department of Commerce to assist in developing voluntary standards to effectively reduce the threat of cyber-risks.” The law also calls for the development of a federal cybersecurity research and development plan.

- New York State’s Department of Financial Services has spelled out a detailed list of issues it will cover in the new cybersecurity portion of its bank examinations. Corporations in general can take useful guidance from this as well. The DFS memo resonates with a variety of legal authorities that call on companies in all sectors of the economy to maintain so-called “reasonable security” – or face legal consequences for failing to do so. Corporations of all types thus must consider this potential double whammy: On the one hand, “reasonable security” may be emerging as a legal standard. On the other hand, no court, regulator or legislature has yet laid out an explicit path to satisfying that standard.

**Telecom**

- The Federal Communications Commission (the FCC) recently took action against two United States telecommunications service providers (the Companies) in the FCC’s first data security case and largest privacy action in the FCC’s history. The FCC is fining the Companies US$10 million for allegedly willfully and repeatedly violating the
Communications Act of 1934. According to the Notice of Liability issued by the FCC on October 24, 2014, after collecting personally identifiable information (PII) from their customers, the Companies:

- “failed to properly protect the confidentiality of their customers’ PII;
- failed to employ reasonable data security practices to protect their customers’ PII; engaged in deceptive and misleading practices by representing to customers in the Companies’ privacy policies that they employed appropriate technologies to protect PII when, in fact, they had not; and engaged in unjust and unreasonable practices by not fully informing customers that their PI had been compromised.”

Worldwide

- On December 22, 2014, the Federal Trade Commission announced that it notified China-based BabyBus (Fujian) Network Technology Co., Ltd., (“BabyBus”) that several of the company’s mobile applications (“apps”) appear to be in violation of the Children’s Online Privacy Protection Rule (the “COPPA Rule”). In a letter dated December 17, 2014, the FTC warned BabyBus of potential COPPA violations stemming from allegations that the company has failed to obtain verifiable parental consent prior to its apps collecting and disclosing the precise geolocation information of users under the age of 13.

Pharmaceuticals

- Bill Ackman has asked for dismissal of the insider-trading lawsuit brought against him by Allergan, Inc., claiming that the Botox-maker cannot sue him as the company was not the one who sold him shares, as reported by Bloomberg.

- China has agreed to streamline its regulatory processes and cut red tape for imports of new drugs, a move that should benefit the U.S. pharmaceutical industry, the U.S. Commerce Department says.

Retail

- Researchers with EMC’s RSA Security Division have pulled back the covers from the Backoff malware in a new report. The Backoff malware made a big splash in the world of cybercrime in 2014, emerging as one of the most notorious pieces of point-of-sale malware in the wild. In August, the U.S. Secret Service linked it to compromises at 1,000 U.S. businesses. It was also linked to attacks on Diary Queen and the United Parcel Service (UPS). The report offers details of the malware’s command and control infrastructure and how it operates. But perhaps more notably, it offers some indication the attacker or attackers controlling the malware may be in India.

- Alibaba Group Holding Ltd., which faced scrutiny for selling counterfeit goods on its websites, said it removed 90 million listings that may have breached intellectual-property rights.

- Following through on threats of a Christmas hack, a Twitter account claiming affiliation with Anonymous released a list of what it says are usernames and passwords for 13,000 accounts on Amazon, PlayStation, XBox Live, Hulu Plus, Walmart and other retail and entertainment services.
Technology

- Chinese access to Google Inc.’s email service has been blocked amid government efforts to limit or possibly ban access to the U.S. company’s services, which are popular among Chinese who seek to avoid government monitoring.

- Facebook Inc., Twitter Inc. and Google Inc. have started resisting Russian government orders to remove information about a rally next month in support of opposition leader Alexei Navalny, raising the prospect of a showdown over the Kremlin’s efforts to control online information. In response to a request from Russian prosecutors, Roskomnadzor, the country’s communications regulator, began issuing block orders for Russia just hours after the Moscow rally was publicized on social media late last week, officials said. Facebook honored the initial order last weekend and blocked a page promoting the event, but others were quickly created, attracting more attention.

- Google and Microsoft have joined a growing chorus of businesses that oppose Marriott's attempt to block guests' Wi-Fi hotspots in their hotel rooms.

Telecommunications

- FairPoint Communications’ pending $13 million contract with New Hampshire has gone into limbo as the state has decided to delay action amidst a spike in service outages that have emerged during a labor strike by its northern New England employees.

- Republican Congressional leaders are proposing a new plan that could prevent service providers from giving priority for some websites over others, reports The Washington Post, citing unnamed industry officials close to the plans.

Defense

- Japan, South Korea, and the United States signed an agreement on December 29, 2014 to share classified information on North Korea's nuclear and missile programs. Under the agreement, South Korea and Japan will pass information to the US Department of Defense, which will then classify it under existing bilateral agreements and share with the other country.

- Russia’s 10-year state rearmament program has reached its halfway point but is only one third completed, the deputy chairman of the government’s military industrial commission has conceded.

- The National Security Agency (NSA) on Christmas Eve released a grip of compliance reports that detail its own admitted failures to always operate inside the orbit of the law. The reports spanned a 12 year period, from 2001 to 2013.

Law Enforcement

- A federal judge has ruled that police can create fake social network profiles on sites such as Facebook and Instagram to search through a suspect's account to use against
them in court. United States District Judge William Martini denied a defendant's motion to suppress evidence collected from his Instagram profile after he connected with an account created by undercover police officers, according to CNN. Judge Martini ruled that the sharing of information was consensual after suspect Daniel Gatson accepted a request to become friends with an undercover officer, enabling law enforcement to view photos and other information that he posted to his Instagram account. As a result, the police did not need a search warrant.

- Google alerted authorities to a Colorado Springs man who threatened to “hunt” and kill police officers in the comment sections of a YouTube video, leading to the man's arrest. Jeremiah M. Perez was arrested after Google contacted the FBI Office in San Francisco. Mr. Perez's threat read, “SINCE DARREN WILSON our group has killed 6 retired sheriffs and cops……because of this event we will hunt two more in colorado this week……for every innocent citizen that cops kill WE, VETERANS WILL KILL RETIRED HELPLESS COPS,” the threat read. “COPS ARE THE REAL ENEMIES OF FREEDOM LOVING AMERICANS and TIME TO STRIKE BACK IN ALL OUT WAR IS NOW.” The user name of the commenter was “Vets Hunting Cops.”

- The Associated Press reports that Homeland Security is beginning to give GPS monitoring bracelets to some parents captured crossing the Mexican border illegal with their children. They were given the devices after being released from custody with notices to report back to immigration officials. According to Homeland Security officials, about 70% of parents fail to report.

- The FBI plans to train 30,000 officers nationwide how to handle an active shooter in schools, businesses and other public places, the USA Today reports. More than 200 agents are helping with the training, which was hatched after the 2012 Newton, Conn., school massacre. The training, which is in partnership with Texas State University, is critical and aimed at shaving time to respond, identify and “eliminate” suspects.

- A former FBI special agent pleaded guilty last week to bribery charges, admitting that he provided internal law enforcement documents and other confidential information about a prominent citizen of Bangladesh for use by a political rival in exchange for cash.