



Homeland
Security

Daily Open Source Infrastructure Report

11 December 2012

Top Stories

- Saudi Arabia's national oil company, Aramco, said December 9 that a cyberattack against it in August that damaged some 30,000 computers was aimed at stopping oil and gas production in Saudi Arabia. The attack on Aramco — which supplies a tenth of the world's oil — was one of the most destructive hacker strikes against a single business. – *Reuters* (See item [1](#))
- Standard Chartered Plc agreed to pay \$327 million of fines after regulators alleged it violated U.S. sanctions with Iran, Bloomberg News reported December 10. – *Bloomberg News* (See item [4](#))
- A spokesman for the Frederick County, Maryland Division of Fire and Rescue Services said December 7 that information was illegally accessed from a company that provides data services for the ambulance service. – *Associated Press* (See item [25](#))
- Security researchers from Carnegie Mellon University, in collaboration with experts from Coherent Navigation, identified new attack vectors against the Global Positioning System (GPS), Softpedia reported December 10. – *Softpedia* (See item [30](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
 - [National Monuments and Icons](#)
-

Energy Sector

1. *December 9, Reuters* – (International) **Saudi Aramco says hackers took aim at its production.** Saudi Arabia's national oil company, Aramco, said December 9 that a cyberattack against it in August that damaged some 30,000 computers was aimed at stopping oil and gas production in Saudi Arabia. The attack on Saudi Aramco — which supplies a tenth of the world's oil — failed to disrupt production, but was one of the most destructive hacker strikes against a single business. Hackers from a group called Cutting Sword of Justice claimed responsibility for the attack, saying that their motives were political and that the virus gave them access to documents from Aramco's computers, which they threatened to release. No documents were published. Aramco and the Saudi Interior Ministry were investigating the attack. A ministry spokesman said the attackers were an organized group operating from countries on four continents. The attack used a computer virus known as Shamoon, which infected workstations on August 15. The company shut its main internal network for more than a week. Shamoon spread through Aramco's network and wiped computers' hard drives clean. Aramco said damage was limited to office computers and did not affect systems software that might harm technical operations.
Source: <http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html>

For another story, see item [20](#)

[\[Return to top\]](#)

Chemical Industry Sector

Nothing to report

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

[\[Return to top\]](#)

Critical Manufacturing Sector

2. *December 10, WYFF 4 Greenville* – (South Carolina) **Flames, heavy smoke destroy plant, close street.** Flames destroyed the Platronics Seals plant in Spartanburg, South Carolina, December 10. A passerby saw smoke and called 9-1-1, dispatchers said. Spartanburg County’s emergency management coordinator was called out because of hazardous chemicals inside the plant. “The area where any chemicals or hazardous materials [are] is separate and not involved in the fire,” he said. He said there was no real danger to the public, but emergency responders were monitoring the water runoff at the site. When crews arrived, heavy flames consumed one side of the building that houses the machine shop and a second floor storage area.
Source: <http://www.wyff4.com/news/local-news/spartanburg-chokeoee-news/Flames-heavy-smoke-destroy-plant-close-street/-/9324158/17714678/-/f7n9s0z/-/index.html>
3. *December 10, U.S. Department of Transportation* – (National) **NHTSA recall notice - 2005-2013 Hino trucks B+ circuit shorting.** Hino announced December 10 the recall of 35,168 model year 2005 through 2013 medium duty trucks, models NA6J, NB6J, NC6J, ND8J, NE8J, NJ8J, NF8J, and NV8J, manufactured from August 18, 2003 through November 16, 2011. Over time, the main B+ circuit from the battery to the starter could potentially short to ground due to wear that accumulates as a result of interference between the B+ circuit and its convoluted tubing sheath. If the B+ circuit shorts to ground, it may lead to a fire. Hino will notify owners, and dealers will repair the vehicles.
Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V555000&summary=true&prod_id=203861&PrintVersion=YES

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Banking and Finance Sector

4. *December 10, Bloomberg News* – (International) **Standard Chartered to pay \$327 million in U.S.-Iran transfers case.** Standard Chartered Plc agreed to pay \$327 million of fines after regulators alleged it violated U.S. sanctions with Iran, Bloomberg

News reported December 10. The bank will pay \$100 million to the Federal Reserve and \$227 million to the U.S. Department of Justice and the District Attorney for New York County. The settlement includes a \$132 million fine to the Treasury Department's Office of Foreign Assets Control, according to a statement from the Federal Reserve. "The orders address unsafe and unsound practices related to inadequate and incomplete responses to examiner inquiries as well as insufficient oversight of its compliance program for U.S. economic sanctions, Bank Secrecy Act, and anti-money-laundering requirements," the Federal Reserve said in the statement. As part of that agreement, the U.S. charged the bank with one count conspiring to violate the International Emergency Economic Powers Act. That charge will be dismissed after two years if Standard Chartered abides by the terms of the agreement, according to court papers.

Source: <http://www.businessweek.com/news/2012-12-10/standard-chartered-pays-327-million-in-u-dot-s-dot-iran-transfers-case>

5. *December 9, KSL-TV 5 Salt Lake City* – (Utah) **2 men used truck to assist in ATM theft, police say.** Police are looking for two people they said pried open the doors at a Murray, Utah gas station and used a pickup truck to steal an ATM December 9. A Murray Police sergeant said a white truck with a utility shell backed up to the entrance of a Tesoro gas station. After forcing the door open, one man entered the store and tied a tow rope to the ATM. The driver of the truck then dragged the ATM out of the store and partway down the street before it was loaded into the vehicle.

Source: <http://www.ksl.com/?sid=23312404&nid=148>

6. *December 8, Reading Eagle* – (Pennsylvania) **4 arrested in bank-cheating check scheme.** Police in Berks County, Pennsylvania, charged a Maryland woman and used a vehicle's GPS tracking system to arrest three other suspects in a State-wide counterfeit-check scheme that stole more than \$100,000 from Metro and Vist Financial banks, the Reading Eagle reported December 8. The scheme, which operated in the Reading, Harrisburg, York, and Philadelphia areas, originated in February. It was led by a Maryland man who drove "runners" to various banks to cash phony checks, police said. Exeter Township police said they arrested one of those runners December 6 on charges she cashed a bogus check at a Metro Bank branch. The man suspected of leading the scheme was stopped by police December 7. Exeter police had learned the man was driving a leased car and were able to track his location by using GPS information provided by the leasing company. Two other suspected runners were also arrested.

Source: <http://readingeagle.com/article.aspx?id=433933>

7. *December 8, Associated Press* – (California) **'Tiger Bandit' bank robber arrested in Calif.** Authorities said a suspected robber dubbed the "Tiger Bandit" implicated himself in five southern California bank heists, the Associated Press reported December 8. Los Angeles County Sheriff's officials said the suspect was arrested December 4 when deputies served a search warrant at a relative's house in Compton. The suspect got his nickname because he was caught in surveillance photos wearing a Detroit Tigers baseball cap. Investigators recovered clothing believed to have been worn during the robberies and some cash. Detectives also seized a car which matched

surveillance video images of the getaway car used during a Santa Monica robbery. The suspect is also linked to bank robberies in Huntington Beach, Marina del Rey, Long Beach, and Lomita since November 23.

Source: <http://www.sfgate.com/news/crime/article/Tiger-Bandit-bank-robber-arrested-in-Calif-4083442.php>

8. *December 7, American Banker* – (International) **Skimming, trapping threatened ATMs in 2012: Survey.** Fraud and physical attacks against ATMs rose globally in 2012, according to a survey of 225 respondents worldwide released December 6 by the ATM Industry Association. According to the survey, the swiping of details embedded in the magnetic stripes of debit and credit cards inserted into ATMs remains the top threat to ATM security, followed by the deployment of devices that trap cash or cards and prevent them from being dispensed to customers. The use of gas and explosives to destroy ATMs increased in the past six months as well, according to the survey. Forty-five percent of those surveyed said criminal attacks on ATMs in their country or region rose since the second quarter, while 53 percent said fraud and attacks on ATMs have added costs to their businesses. Roughly 54 percent of respondents said they invested more in security technology compared with six months ago, while 42 percent report no change in their investment.

Source: http://www.americanbanker.com/issues/177_235/skimming-trapping-threatened-atms-in-2012-survey-1055023-1.html

9. *December 7, U.S. Securities and Exchange Commission* – (Florida) **SEC charges prominent entrepreneur in Miami-based scheme.** The U.S. Securities and Exchange Commission (SEC) December 7 charged a prominent Miami-based entrepreneur with defrauding investors by grossly exaggerating the financial success of his company that purportedly produced housing materials to withstand fires and hurricanes. The man stole at least \$8.1 million, nearly half of the money raised from investors, to pay for various luxury expenses. The SEC alleges that the man raised at least \$16.8 million from investors by portraying InnoVida Holdings LLC as having millions of dollars more in cash and equity than it actually did. To add an air of legitimacy to his company, he assembled a high-profile board of directors that included a former governor of Florida, a lobbyist, and a major real estate developer. He falsely told a potential investor he had invested tens of millions of dollars of his own money as InnoVida's largest stakeholder, and he hyped a Middle Eastern sovereign wealth fund investment as a ruse to solicit additional funds from investors. The SEC also charged InnoVida's chief financial officer, a certified public accountant living in Pembroke Pines, who helped the man create the false financial picture of InnoVida.

Source: <http://www.sec.gov/news/press/2012/2012-258.htm>

For more stories, see items [25](#), [27](#), and [29](#)

[\[Return to top\]](#)

Transportation Sector

10. *December 10, Associated Press* – (Ohio) **Victim identified in Ohio airport murder-suicide.** The medical examiner's office released the identity of the victim in a murder-suicide in an employee parking lot at Cleveland Hopkins International Airport, the Associated Press reported December 10. The shooting occurred at a lot north of the airport in an industrial area along Interstate 480. Police said a man fatally shot his wife — a Transportation Security Administration (TSA) officer — before shooting himself. The wife and a second TSA employee were commuting to work. Police said the husband apparently followed her to the off-site lot, blocked her in her car with his vehicle and began firing. Police said he fired at the other TSA agent but missed. Source: <http://www.sfgate.com/news/crime/article/Shooter-identified-in-Ohio-airport-murder-suicide-4104735.php>
11. *December 10, Sioux Falls Argus Leader* – (South Dakota) **Wintry weather closes roads.** Gusty winds and freezing road surfaces forced South Dakota's two major Interstates to close December 9 as motorists faced long waits in their vehicles or at truck stops. Drifting and visibility concerns caused South Dakota Department of Transportation officials to close Interstate 90 from Chamberlain to Sioux Falls, and Interstate 29 from Sisseton to Sioux Falls. At mid-afternoon, motorists diverted off the interstate at Brookings were finding hotel rooms in short supply. Many crammed into places such as BP-Amoco to wait for the road to be opened again. I-90 was open State-wide by December 9, but I-29 reopened only from Sisseton to Watertown; it was expected to be open to Sioux Falls sometime December 10. At the Sioux Falls Regional Airport, a United flight scheduled to arrive from Chicago was canceled, as was a departing United flight back to Chicago. Several other flights had minor delays. Source: <http://www.argusleader.com/article/20121210/NEWS/312100011/Wintry-weather-closes-roads?odyssey=nav|head>
12. *December 10, Associated Press* – (New Mexico) **Heavy snow in NM sparks delays, 1 fatal crash.** Heavy snows and icy roads left parts of New Mexico with forced delays, dangerous driving conditions, and at least one person dead, the Associated Press reported December 10. A number of schools and schools districts were closed as well. New Mexico State Police said at least one person was killed December 9 in a weather-related car crash near Waldo, forcing the temporarily closure of Interstate 25 just south of Santa Fe. The winter storm, which struck northern and central areas of the State, also forced the temporary closure of Interstate 40 in Clines Corners where two semi-trucks were jack knifed. Both highways were reopened as of December 10, but State transportation officials urged motorists to use extreme caution and expect heavy delays. The winter weather forced some northern New Mexico cities and towns to open on a two-hour delay December 10. Source: <http://www.kob.com/article/stories/s2861116.shtml>
13. *December 9, Lincoln Journal Star* – (Utah) **Computer network disruption delays SkyWest flights.** SkyWest Airlines said a disruption in its computer network kept its flights throughout the country from taking off for about 2 hours. A spokeswoman said the system went down December 9 and was restored. She said that service from the

airline's network provider was disrupted. That kept pilots from getting information about planes including fuel amounts, weight, and balance. Ongoing delays of 90 minutes to 2 hours were expected on flights throughout the day. SkyWest is a Utah-based carrier that services flights for United, Delta, US Airways, American Airlines, and others.

Source: http://journalstar.com/news/national/computer-network-disruption-delays-skywest-flights/article_257f195a-a70d-5d7b-aa59-dae6568be4a3.html

14. *December 9, United Press International* – (Minnesota) **Up to 17 inches of snow coats Minnesota.** A big winter storm dumped 17.3 inches of snow on Sacred Heart Minnesota, December 9, and caused problems for motorists in the Twin Cities, meteorologists said. Sacred Heart recorded 17.3 inches of snow, and winds were blowing it around, reducing visibility. Minneapolis and St. Paul received about a foot. The St. Paul Pioneer Press reported the Minnesota State Patrol said more than 300 collisions were reported, with 32 injuries, since December 8. Another 330 vehicles slid off the road or spun out. The Minneapolis Star Tribune said there had been one storm-related traffic fatality involving a tractor-trailer rig near Red Wing. Several dozen flights were canceled at the Minneapolis-St. Paul airport. The Star Tribune said snow emergencies and parking restrictions had been declared for the Twin Cities and Plymouth, Bloomington, Golden Valley, Mendota Heights, St. Louis Park, and St. Cloud.

Source: http://www.upi.com/Top_News/US/2012/12/09/Up-to-17-inches-of-snow-coats-Minnesota/UPI-23611355075790/

For another story, see item [30](#)

[\[Return to top\]](#)

Postal and Shipping Sector

15. *December 10, Associated Press* – (Mississippi) **Chatawa Post Office operations suspended.** The Associated Press reported December 10 that a U.S. Postal Service spokesman stated that the Chatawa Post Office in Pike County, Mississippi, closed indefinitely because of structural damage it received from flooding from Hurricane Isaac. She had no information on if or when the office will reopen. The action comes as no surprise for some residents, who said the threat of a closure has been looming over the office at least 5 years. The 29 customers who received their mail at post office boxes in Chatawa now must go to Osyka to get their mail.

Source: <http://www.seattlepi.com/news/article/Chatawa-Post-Office-operations-suspended-4104621.php>

[\[Return to top\]](#)

Agriculture and Food Sector

16. *December 9, Associated Press* – (International) **USDA relists Canadian meatpacking plant.** The Canadian Food Inspection Agency (CFIA) reported December 7 that the

U.S Department of Agriculture (USDA) relisted the XL Foods plant in Brooks, Alberta, Canada, since it revoked the plant's permit to export beef to the U.S. September 13. CFIA revoked the plant's permit at the request of the USDA after several of the company's beef products were recalled due to contaminated E. coli beef.

Source:

<http://www.google.com/hostednews/ap/article/ALeqM5hxwJ2ZT5jK8XPxYi09OEK5AgIIjQ?docId=91a388abbcec4fde9e89e0022b0bf69c>

17. *December 7, U.S. Food and Drug Administration* – (International) **LifeVantage Corporation announces voluntary recall and replacement of select lots of Protandim dietary supplement due to potential health risk.** LifeVantage Corporation announced December 7 that it contacted affected independent distributors and other customers to voluntarily recall and replace bottles of its Protandim, the Nrf2 Synergizer, dietary supplement because of possible inclusion of small metal fragments in the final product. The fragments were originally discovered in batches of turmeric extract, an ingredient in Protandim that was purchased from a third party supplier. Protandim is packaged in a cylindrical blue bottle and contains thirty caplets per bottle. Affected Protandim lots were distributed in the United States and Japan between July and November 2012. Lot numbers are located on the left side of the product label when looking at the front of the label, directly above the RFID scan bar. When the company was alerted to this issue, it immediately isolated affected product and began working with its third party manufacturers, suppliers, and industry experts to mitigate any health risk potential.

Source: <http://www.fda.gov/Safety/Recalls/ucm331258.htm>

18. *December 7, U.S. Department of Agriculture Food Safety and Inspection Service* – (National) **Consumers, industry benefit under FSIS hold and test implementation.** The U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) December 7 announced that, beginning in 60 days, the Agency will require producers to hold shipments of non-intact raw beef and all ready-to-eat products containing meat and poultry until they pass testing for foodborne adulterants. The new policy requires official establishments and importers of record to maintain control of products tested for adulterants by FSIS and not allow the products to enter commerce until negative test results are received. FSIS anticipates most negative test results will be determined within two days. The policy applies to non-intact raw beef products or intact raw beef products intended for non-intact use and that are tested by FSIS for Shiga-toxin producing Escherichia coli. Also, the policy applies to any ready-to-eat products tested by FSIS for pathogens.

Source: http://www.fsis.usda.gov/News_&_Events/NR_120712_01/index.asp

[\[Return to top\]](#)

Water Sector

19. *December 10, Salisbury Daily Times* – (Maryland) **Md. eyes Sandy sewage spills.** Nearly 3 million gallons of untreated sewage spilled into Lower Shore rivers in Maryland during superstorm Sandy, the Salisbury Daily Times reported December 10.

All of the marred waterways – the Manokin, Pocomoke, and Wicomico rivers – flow into the Chesapeake Bay, itself the subject of a multi-State, multibillion-dollar environmental cleanup. In all of the cases, the untreated sewage was diluted by heavy doses of storm water. The largest spill was at the Snow Hill Wastewater Treatment Facility. The plant became engulfed in the Pocomoke’s rising waters. By the time the water receded, 2.4 million gallons of untreated sewage had washed into the river. As the water rose the night of October 29, the plant manager shut down the new section of the plant, leaving the old portion to handle the river water and sewage alone. The Maryland Department of the Environment (MDE) received at least 99 reports of overflows that involved raw or partially treated sewage for a total of more than 76 million gallons. That was better than 2011’s combination of Hurricane Irene and Tropical Storm Lee, which left 187 spills and 218 million gallons of sewage in their wake, said an MDE spokesman.

Source: <http://www.delawareonline.com/article/20121210/NEWS08/312100050/Md-eyes-Sandy-sewage-spills?odyssey=mod|newswell|text|Home|s>

20. *December 9, Denver Post* – (Colorado) **Drilling spills reaching Colorado groundwater; State mulls test rules.** Oil and gas contaminated groundwater in 17 percent of the 2,078 spills and slow releases that companies reported to Colorado regulators over the past 5 years, State data showed. The damage was worse in Weld County, where 40 percent of spills reach groundwater, the Denver Post reported December 9. Most of the spills happened less than 30 feet underground — not in the deep well bores that carry drilling fluids into rock. State regulators said oil and gas crews typically worked on storage tanks or pipelines when they discover that petroleum material, which can contain cancer-causing benzene, has seeped into soil and reached groundwater. Companies respond with vacuum trucks or by excavating tainted soil. Contamination of groundwater — along with air emissions, truck traffic, and changed landscapes — has spurred public concerns about drilling along Colorado’s Front Range. There are 49,236 active wells State-wide, up 31 percent since 2008, with 17,844 in Weld County. Colorado Oil and Gas Conservation Commission (COGCC) regulators that struggled to maintain a consistent set of State rules governing the industry would discuss with the groundwater issue December 10. The COGCC considered proposed changes to State rules that would require companies to conduct before-and-after testing of groundwater around wells to provide baseline data that could be used to hold companies accountable for pollution.
- Source: http://www.denverpost.com/environment/ci_22154751/drilling-spills-reaching-colorado-groundwater-state-mulls-test

21. *December 7, WBNS 10 Columbus* – (Ohio) **Mansfield residents warned of chemicals found in well water.** The Ohio Department of Health detected the chemicals TCE, and “one and two DCE” in the well water serving the Madison Early Childhood Learning Center in Mansfield, WBNS 10 Columbus reported December 7. It prompted them to call in the Ohio Environmental Protection Agency (EPA) to check 30 private wells nearby. The environmental health director with the local health department said that TCE can have long-term damaging effects. “It can cause problems with the liver and the lungs,” he said. A team from the Ohio EPA collected samples from wells over the week of December 3 and December 6. As families waited for results, health

department officials recommended they use bottled water for cooking and drinking.
Source: <http://www.10tv.com/content/stories/2012/12/07/mansfield-residents-warned-chemicals-in-well-water.html>

[\[Return to top\]](#)

Public Health and Healthcare Sector

22. *December 10, Atlantic Information Services* – (Maryland) **Health Plan’s \$3 million fine for accessing Medicare files shows new fed muscle.** The Maryland-based Coventry Health Care, Inc. agreed to pay the U.S. Department of Justice (DOJ) \$3 million to avoid prosecution for any “crimes arising” from unauthorized employees dipping into Medicare’s beneficiary database, which they apparently did with the knowledge of a number of senior managers, the Atlantic Information Services reported December 10. The DOJ alleged workers “inappropriately accessed the Medicare database to obtain Medicare eligibility information for the sale of Medicare set-aside products.” Workers who accessed the database, which DOJ described as “password protected,” were apparently part of First Health, the firm’s workers compensation division. Coventry purchased First Health’s workers comp business in 2005. According to the settlement agreement, the unauthorized access began in May 2005 and was committed by “some” Coventry workers and/or First Health Priority Services. It continued for some 18 months. In forging the agreement, the DOJ shut down potential actions by any other agencies, agreeing it would not “refer this matter to the Department of Health and Human Services for administrative review” nor bring any new “civil, criminal or administrative cause” against the plan, which has 5 million members, including 1.4 million Medicare drug benefit policy holders. The agreement and steep payment show the use of a new avenue for federal enforcement and penalties for patient privacy, security, and access issues, and demonstrates that a high price can be exacted even when HIPAA is not invoked.
Source: <http://aishealth.com/archive/hipaa1212-02>
23. *December 8, Los Angeles Times* – (California) **Surgeon infected patients during heart procedure, Cedars-Sinai admits.** A heart surgeon at Cedars-Sinai Medical Center in Los Angeles unwittingly infected five patients during valve replacement surgeries earlier this year, causing four of the patients to need a second operation, the Los Angeles Times reported December 8. The infections occurred after tiny tears in the latex surgical gloves routinely worn by the doctor allowed bacteria from a skin inflammation on his hand to pass into the patients’ hearts, according to the hospital. The patients survived the second operation and are still recovering, hospital officials said. The outbreak led to investigations by the hospital and both the Los Angeles County and California departments of public health. The federal Centers for Disease Control and Prevention was also consulted.
Source: <http://www.latimes.com/news/local/la-me-cedars-infections-20121208,0,3931111.story>

[\[Return to top\]](#)

Government Facilities Sector

24. *December 7, Associated Press* – (Mississippi) **Man enters plea in federal threat case.** A man pleaded guilty to threatening agents working in the Hattiesburg, Mississippi office of the FBI. A U.S. Attorney said he entered the plea December 6 in federal court in Hattiesburg. The suspect admitted that he posted an email message on the FBI's national Web site September 18 in which he threatened to go to the "little FBI office in Hattiesburg, Mississippi and start putting some bullets through the heads of people."
Source: <http://www.sunherald.com/2012/12/07/4346050/man-enters-plea-in-federal-threat.html>

For more stories, see items [12](#), [22](#), and [30](#)

[\[Return to top\]](#)

Emergency Services Sector

25. *December 7, Associated Press* – (Maryland) **Information from ambulance billing stolen.** Frederick County, Maryland's rescue service said account information from the ambulance billing system was stolen and given to a theft ring. A spokesman for the Frederick County Division of Fire and Rescue Services said December 7 that the company which provides data services for the ambulance service learned in October that information had been illegally accessed. The company, Advanced Data Processing Inc., said some individual account information had been disclosed to a theft ring suspected of filing fraudulent federal tax returns. The theft included ambulance data from Frederick County and First Response Medical Transportation Corp. Advanced Data Processing said it notified people that were affected.
Source: <http://www.sfgate.com/news/crime/article/Information-from-ambulance-billing-stolen-4100280.php>

For another story, see item [30](#)

[\[Return to top\]](#)

Information Technology Sector

26. *December 10, Softpedia* – (International) **Exforel backdoor implemented at NDIS level to be more stealthy.** Security researchers from Microsoft's Malware Protection Center have identified a variant of the Exforel backdoor malware, VirTool:WinNT/Exforel.A, that is somewhat different from other malicious elements of this kind. The backdoor is implemented at the Network Driver Interface Specification (NDIS) level. Since Exforel.A implements a private TCP/IP stack and hooks NDIS_OPEN_BLOCK for the TCP/IP protocol, the backdoor TCP traffic is diverted to the private TCP/IP stack and then delivered to the backdoor. This makes this variant of the malware more low-level and stealthy because there is no connecting

or listening port. Furthermore, the backdoor traffic is invisible to user-mode applications. According to experts, this particular version of Exforel – which can download, upload, and execute files, and rout TCP/IP packets – is used in a targeted attack against a particular organization.

Source: <http://news.softpedia.com/news/Exforel-Backdoor-Implemented-at-NDIS-Level-to-Be-More-Stealthy-Experts-Say-313567.shtml>

27. *December 10, Help Net Security* – (International) **Beware of Bitcoin miner posing as Trend Micro AV.** Trend Micro researchers recently uncovered a piece of malware that tried to pass itself off as “Trend Micro AntiVirus Plus AntiSpyware”. The software in question is a trojan that creates the process svchost.exe and downloads additional malicious components such as a Bitcoin miner application created by Ufasoft. This particular application will, unbeknownst to the victim, use the infected system’s resources to create Bitcoins for the people behind this scheme. “This attack is timely because of the news that Bitcoin Central has been approved by the law to function as a bank where exchange from Euro and Bitcoins are now possible,” the researchers noted. Source: [http://www.net-security.org/malware_news.php?id=2349&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+\(Help+Net+Security\)&utm_content=Google+Reader](http://www.net-security.org/malware_news.php?id=2349&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader)
28. *December 9, Associated Press* – (International) **Ex-Idaho woman hiding after \$163m federal judgment.** A former Idaho woman believed to be hiding out in the Caribbean owes the U.S. government \$163 million, part of a federal civil judgment earlier this year stemming from an Internet scam, the Associated Press reported December 9. According to the Federal Trade Commission (FTC), she participated in an Internet scheme in which people were frightened into buying virus-protection software they did not need. Others involved in the business, called Innovative Marketing, paid some \$16 million in settlements. But the woman from Idaho remains at large, possibly on the Caribbean island of Nevis. Her former boyfriend is also an international fugitive targeted by the FBI’s cybercrimes unit. Innovative Marketing pushed advertisements that claimed users had hundreds of viruses or illegal files that needed cleansing and offered software for \$39.95 or more. But installing the product did not help; it gave the user more scareware ads, according to the FTC. Source: <http://www.foxreno.com/news/ap/crime/ex-idaho-woman-hiding-after-163m-federal-judgment/nTQ95/>
29. *December 8, PC World* – (Texas) **Anonymous affiliate indicted for threats, stolen credit cards.** A federal grand jury in Dallas indicted a putative spokesman for the hacker collective known as Anonymous in connection with a massive data breach of Stratfor Global Intelligence. The man is in federal prison based on another indictment returned against him October 3. In that case he was charged with making a threat on the Internet, conspiring to make public restricted personal information of a federal employee, and retaliation against a federal law enforcement officer. One of the crimes he is accused of in the indictment is transferring a hyperlink from an Internet Relay Chat (IRC) channel apparently occupied by Anonymous to a channel controlled by himself. The hyperlink provided access to data stolen from Stratfor, which included

more than 5000 credit card account numbers, information about their owners, and their Card Verification Values (CVV). By transferring and posting the hyperlink to the Internet, the man caused the data to be made available to persons online without the knowledge and authorization of Stratfor or the cardholders. He is also charged with possession of at least 15 credit card numbers and their CVV codes without the knowledge of the cardholders with intent to defraud them. In addition, the indictment accuses him of aggravated identity theft by knowingly transferring and possessing without lawful authority the means of identification of the credit card holders.

Source: <http://www.pcworld.com/article/2019242/anonymous-affiliate-indicted-for-threats-stolen-credit-cards.html>

For more stories, see items [13](#) and [30](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <https://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

30. *December 10, Softpedia* – (National) **GPS software attacks more dangerous than jamming and spoofing, experts say.** Security researchers from Carnegie Mellon University, in collaboration with experts from Coherent Navigation, identified new attack vectors against the Global Positioning System (GPS), Softpedia reported December 10. According to the researchers, a malicious 45-second GPS broadcast is capable of taking down more than 30 percent of the Continually Operating Reference Station (CORS) network, which is used for safety and life-critical applications. Furthermore, it could also disrupt 20 percent of the Networked Transport of RTCM via Internet Protocol (NTRIP) systems. A total of three new attack methods have been identified: GPS data level attacks, GPS receiver software attacks, and GPS dependent system attacks. GPS data level attacks are somewhat similar to spoofing, but they can cause more damage. For instance, such an attack can remotely crash a high-end receiver. The second type of attacks leverages the fact that GPS receivers run some kind of computer software that can be remotely compromised. Since GPS receivers are most often seen as devices instead of computers, the security holes leveraged by attackers can remain unpatched for extended periods of time. In order to mitigate such threats, experts recommend stronger verification of GPS receiver software and the deployment of regular software updates for IP-enabled devices. Another mitigation strategy refers to the use of Electronic GPS Attack Detection System (EGADS) that alerts users when an attack is underway, and an Electronic GPS Whitening System (EGWS) that re-broadcasts a whitened signal to otherwise vulnerable receivers. One noteworthy thing about these types of attacks is that they do not require sophisticated or

expensive equipment. The hardware utilized by the researchers costs only about \$2,500.

Source: <http://news.softpedia.com/news/GPS-Software-Attacks-More-Dangerous-Than-Jamming-and-Spoofing-Experts-Say-313388.shtml>

31. *December 10, Lower Providence Patch* – (Pennsylvania) **Police: Over \$22,000 worth of copper cables stolen in Audubon.** Lower Providence, Pennsylvania police reported that five copper power cables, worth over \$22,000, were stolen from the Sprint/Nextel parking lot in Audubon. The incident was reported December 4 by a Sprint/Nextel switch technician. The technician told police that the cables were stolen from portable generators left on the property. According to police, at the time of the report two Olympian generators and three Generac generators were returned to the business and placed in its parking lot, with the power cables attached and in working order. The approximate value of each cable is \$4,500.

Source: <http://lowerprovidence.patch.com/articles/police-over-22-000-worth-of-copper-cables-stolen-in-audubon>

[\[Return to top\]](#)

Commercial Facilities Sector

32. *December 10, KABC 7 Los Angeles* – (California) **Commercial building catches on fire in Vernon.** A commercial building that houses three businesses in Los Angeles caught on fire December 9. The second alarm fire was reported in the Vernon district of the city. More than 50 firefighters responded to the scene. The building was evacuated and there were no reports of injuries. The extent of damage was not immediately known, but a partial roof collapse was reported.

Source:

http://abclocal.go.com/kabc/story?section=news/local/los_angeles&id=8914531

33. *December 10, WYMT 57 Mountain News* – (Tennessee) **Campbell County, TN church destroyed by fire.** The Fincastle Church of God in LaFollette, Tennessee, was engulfed in flames and destroyed December 9. The Campbell County Sheriff's Department drove by and noticed smoke coming from the church. Firefighters arrived within minutes and continually pushed back flames throughout the night. Multiple fire stations had to be called to fight the fire. No nearby fire hydrants were found, so water was trucked in to fight the fire. Officials said the fire started in the basement. Officials were continuing to investigate whether arson was involved.

Source: <http://www.wkyt.com/wymt/home/headlines/Campbell-County-TN-church-destroyed-by-fire-182797471.html>

34. *December 10, WRTV 6 Indianapolis* – (Indiana) **7-year-old boy killed, 5 injured in Indianapolis apartment fire.** One person was killed December 8 in a fire on Indianapolis' west side. When Indianapolis Fire Department firefighters arrived, they found flames shooting from the second floor of the building. The fire was brought under control within 30 minutes in the building that contained 5 apartment units and 16 residents. The officers who were first to arrive at the fire encountered "heavy fire and

frantic residents evacuating, jumping from the building,” an Indianapolis Fire Department captain said. Five adults were taken to a local hospital for treatment of minor injuries, and one firefighter suffered steam burns to his face and legs. Fire crews said there were no working smoke detectors in the apartment building, and that damage was estimated at \$150,000.

Source: <http://www.theindychannel.com/news/local-news/7-year-old-boy-killed-5-injured-in-indianapolis-apartment-fire>

35. *December 10, WFOR 4 Miami* – (Florida) **Police ID man, woman in Sunrise church shooting.** Sunrise Police officers investigated a shooting and suicide outside a church December 9 in Fort Lauderdale, Florida. Multiple shots were fired outside the Faith Center Church police said. Witnesses said the church was packed with more than a thousand people. Investigators said the shooter waited for the victim, his ex-girlfriend, outside. According to the detectives, the man then turned the gun on himself. They said the woman managed to drive away. Police said the gunman died at the hospital. The victim was being treated at a local medical center.

Source: <http://miami.cbslocal.com/2012/12/10/woman-injured-in-shooting-outside-sunrise-church/>

36. *December 9, Houston Chronicle* – (Texas) **1 killed, 4 hurt in violence at FM 1960 after-hours club.** Four people were shot, one fatally, December 9 outside an after-hours club in northwest Harris County, Texas. The club was the site of several previous shootings. One victim died at the strip mall at a nearby intersection. Four others were transported to area hospitals, said a sergeant with the Sheriff’s Office homicide division. Crime scene officers cataloged at least 15 casings from two different handguns, working around a patrol car that lost its front bumper when ramming a shooting suspect’s car at the same location the week of December 3. About 600 people were inside the club when the shooting took place, and the fire marshal was conducting an investigation into possible violations for overcrowding.

Source: <http://www.chron.com/news/houston-texas/houston/article/1-killed-4-hurt-in-violence-at-FM-1960-4103335.php>

37. *December 8, New England Cable News* – (Massachusetts) **8 people hospitalized after carbon monoxide leak in Boston.** A yoga studio and spa in downtown Boston remained open December 8, despite an earlier carbon monoxide scare. Boston EMS received a call that some employees and patrons there felt lightheaded. When they arrived, even more people had become sick, so they called in the Boston Fire Department. “[The victims had] pretty typical symptoms of carbon monoxide poisoning or higher levels of carbon monoxide in their blood,” said the Boston deputy fire chief. More than 30 people were sickened, and a total of 8 were taken to local hospitals. Fire crews quickly tested the air in the spa. Fire officials believed the four large gas-powered clothes dryers, used to dry the spa’s towels, caused the leak. Spas are required to have the ventilation system cleaned annually, but they are not required to have it certified as restaurants are. Unlike residential buildings, commercial buildings are not required to have carbon monoxide detectors.

Source: <http://www.necn.com/12/08/12/-8-people-hospitalized-after-carbon-mono/landing.html?blockID=811481&feedID=11106>

For another story, see item [29](#)

[\[Return to top\]](#)

National Monuments and Icons Sector

Nothing to report

[\[Return to top\]](#)

Dams Sector

38. *December 10, Delaware News Journal* – (Delaware) **New Castle levees under scrutiny.** Coastal dikes in northern Delaware survived superstorm Sandy without major breaches, but officials got a preview of just how vulnerable the levees could be during the catastrophic weather, the Delaware New Journal reported December 10. Pounding surf and tides eroded chunks of the earthen structures, depositing mounds of debris on them and uprooting trees during the storm that struck the Atlantic coastline in late October. Crews filled in the cut-away areas with riprap and reinforced weakened areas with 200 one-ton bags of sand, but the damage – estimated at nearly \$3.57 million – prompted leaders to bump up a series of refurbishment projects, previously expected to roll out over several years. Five large dikes protect low-lying areas from New Castle to near Delaware City by providing a barrier between the surging tides of the Delaware River and nearby homes, businesses, and public infrastructure. In New Castle, four dikes protect miles of roadway, more than 80 structures, and help prevent upstream flooding during lengthy storms. The Delaware General Assembly already set aside \$4.5 million for part of the dike project, which is likely eligible for another \$3.5 million in federal Sandy-recovery funds, according to the Delaware Department of Natural Resources and Environmental Control (DNREC). As part of the State’s next fiscal budget, the DNREC secretary requested another \$2.5 million in capital funds from the general assembly for the dikes and repairs to high-hazard dams. Officials were optimistic that that funding, together with federal storm-recovery aid, would provide enough to cover dike refurbishment and storm-damage costs.

Source: <http://www.delawareonline.com/article/20121210/NEWS08/312100042/New-Castle-levees-under-scrutiny?odyssey=tab|topnews|text|Home>

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2341

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.