



Homeland Security

Daily Open Source Infrastructure Report for 17 May 2010

Current Nationwide Threat Level

ELEVATED



Significant Risk of Terrorist Attacks

For information, click here:
<http://www.dhs.gov>

Top Stories

- According to DarkReading, a targeted malware attack aimed at human resources departments and hiring managers in the United States and Europe sent 250,000 e-mails during a four-hour period May 12. Researchers at Websense Security Labs discovered the attack, which included the subject line “New resume.” (See item [52](#))
- The Peoria Journal Star reports that heavy rains in Fulton County, Illinois caused one levee to break May 13, and London Mills residents were being cautioned about the rising Spoon River. (See item [64](#))

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

Current Electricity Sector Threat Alert Levels: **Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - <http://www.esisac.com>]

1. *May 14, Associated Press* – (Louisiana) **BP’s next try to stem oil gusher: Smaller tube.** BP officials said May 13 they would thread a small tube into a jagged pipe on the seafloor to suck oil to the surface before it can spew into the Gulf of Mexico and add to a disaster apparently set in motion by a long list of equipment failures. Engineers will have to make sure the 6-inch-wide tube is inserted deep enough into the 21-inch-wide

pipe so gas and seawater do not mix, which can form crystals that could clog the tube. They will also have to thread the tube into the pipe without hitting debris around the riser. The smaller tube will be surrounded by a stopper to keep oil from leaking into the sea. The tube will then siphon the crude to a tanker at the surface, though BP declined to estimate how much oil the tube would be able to collect. A company spokesman said engineers hope to start moving the tube into place Thursday night, but it will take 12 hours to get the tube fully hooked up. Another option is a small containment box called a “top hat,” which is already on the seafloor and also would siphon oil to a tanker on the surface. Officials are waiting on trying to use the box until they know if the tube works, and how well it is working, he said. Engineers still might consider trying to fill the leak with golf balls and other debris — the “junk shot,” though that will not be until at least next week. And a relief well is being drilled, but completion is at least two months away.

Source:

<http://www.themorningsun.com/articles/2010/05/14/business/srv0000008267179.txt>

2. *May 14, News Tribune (Tacoma)* – (Alaska) **Shell tweaks Arctic oil spill safeguards.** Shell executives in Alaska are under massive pressure to prove to federal regulators by early next week that their plan to drill in Arctic waters this summer will not result in an oil disaster like the one unfolding in the Gulf of Mexico. The executives are drafting a letter to the head of the federal Minerals Management Service (MMS) proposing additional measures the company will take to safeguard against a major oil spill. Those proposals have not been fully vetted internally at Shell, but they will likely involve additional testing of undersea well equipment, reducing the response time for a backup drill rig to arrive in an emergency from the Canadian or U.S. Arctic, and increasing the remote-controlled devices and steel barriers used to seal a well during an emergency, company officials said May 13. The Department of the Interior, which has already canceled some planned oil lease sales in Lower 48 waters in the wake of BP’s Gulf of Mexico spill, put Shell on notice a week ago that it falls under a temporary halt to all offshore drilling proposals in the United States. The department also announced it will not rule on the company’s drill permit until a MMS safety review, due to the White House by May 28, is evaluated. During a two-and-a-half hour session with Daily News reporters this week, top Shell managers described the procedures and equipment they use to prevent well blowouts like the one that destroyed the Deepwater Horizon rig in the Gulf and led to an immense leak that is pouring tens of thousands of gallons of oil per day into the ocean.

Source: <http://www.thenewstribune.com/2010/05/13/1185766/shell-tweaks-chukchi-spill-safeguards.html>

3. *May 13, Oakland Tribune* – (California) **Newark oil refinery fire burned for 90 minutes.** More than 60 firefighters, including those from Fremont and Union City, were called to Evergreen Oil refinery in Newark, California May 13, to extinguish a three-alarm fire that was contained to the plant’s five-story heater stack. Firefighters doused the flames at the Smith Avenue complex for nearly an hour and a half before they were fully extinguished. The blaze, which was reported about 12:45 a.m., damaged only the heater stack and did not require the plant to shut down, said a

spokeswoman for the Alameda County Fire Department. Refinery officials told firefighters during the blaze that a petroleum-based fluid appeared to catch fire inside the stack. Fire crews checked air quality during the incident and determined that a “shelter in place” was not needed.

Source: http://www.mercurynews.com/breaking-news/ci_15071641?nclick_check=1

4. *May 13, NBC Connecticut* – (Connecticut) **Underground fire knocks out power in New Haven.** The power was out for about 750 homes and businesses in New Haven after an underground fire on May 13. An electrical fire started in an underground transformer vault in front of 247 College Street and sent smoke spewing above ground. Firefighters were able to contain it so it did not spread to other buildings, but the fire did spark a secondary blaze on Crown Street. Several streets were closed down as firefighters investigated and power outages affected homes and businesses, including the Schubert Theater and Taft apartments. The cause could be a utility vault, according to the New Haven Fire Department, but that has not been confirmed. The fire also closed College Street. Investigators and a crew from United Illuminating were at the scene.

Source: <http://www.nbcconnecticut.com/news/local-beat/Underground-Fire-Closes-College-Street-in-New-Haven-93665934.html>

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

Chemical Industry Sector

5. *May 14, Associated Press* – (Connecticut) **Cleanup continues in Conn. train derailment.** Officials are questioning the safety of a stretch of tracks in eastern Connecticut where trains hauling hazardous substances have derailed twice this spring. Cleanup continued May 14 at the site of the latest derailment, which occurred May 12 in Lisbon. Crews were trying to repair broken lengths of track and stand the nine derailed cars upright again. The Governor says they want details on whether the privately owned tracks are safe and being properly maintained. A portion of Route 12 remained closed May 14 because of the cleanup work. The Providence & Worcester Railroad train was carrying liquid latex. Another train from that company was carrying ethanol when it derailed in March in Windham. No injuries were reported in either incident.

Source: <http://www.courant.com/news/local/statewire/hc-ap-ct-trainderailmentmay14,0,3316384.story>

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

Nuclear Reactors, Materials and Waste Sector

6. *May 14, Rutland Herald* – (Vermont) **State wants Yankee to speed up soil tests.** The Vermont Department of Health (VDH) says Entergy Nuclear is dragging its feet testing soil contaminated with radioactive isotope strontium-90, a more dangerous isotope than the tritium that is suspected of being in the soil under the leaky pipe tunnel at Vermont

Yankee. The radiological health chief for VDH said he knew the samples had been taken because people from the state had witnessed them and labeled them. "I have seen them in the north warehouse awaiting shipment. I do not know specifically why they are lagging behind," the health official wrote in an e-mail. The health official said he had asked Vermont Yankee and Entergy officials for more than six weeks for the samples, but so far they have not been given to him. "We have always had challenges getting radioactive samples out of VY in a timely manner," he noted. VDH had reported on its Web site March 30 that Entergy and the state "are sending samples" to different labs to be tested. Strontium-90 requires a different test than the other radioactive isotopes found at the plant. The health official said he had been told the strontium-90 samples would finally be shipped out to the state's lab this week. "We are pressuring VY to get more samples out now, and get all of them out to our labs faster after they are obtained," the health official said.

Source:

<http://www.rutlandherald.com/article/20100514/NEWS02/5140368/1003/NEWS02>

7. *May 13, Brattleboro Reformer* – (Vermont) **VY decommissioning fund at all-time high.** The decommissioning trust fund set aside for the eventual cleanup of the site of Vermont Yankee nuclear power plant in Vernon, Vermont hit an all-time high of nearly \$452 million by the end of April. At its previous highest level, in September 2007, the trust fund contained \$440 million. But after the stock market crashed in October 2007, the fund fell to \$347 million. By March of this year, 16 months after the crash, the fund had recouped its losses and then some, reaching \$445 million. The decommissioning costs of the power plant have been estimated at between \$600 million and \$1 billion. The low number is the cost of remediating the site to Nuclear Regulatory Commission (NRC) standards. The high number is the estimated cost of cleaning up the site to state standards. The decommissioning fund was created through a surcharge on the electric bills of Vermonters. The surcharge was discontinued after Entergy bought the plant in 2002 from a consortium of public utilities, known as the Vermont Yankee Nuclear Power Corp., which included Central Vermont Public Service, Green Mountain Power and Public Service of New Hampshire. Entergy has not made any contributions to the decommissioning fund, but in January it supplied a \$40-million "parental guarantee" to ensure the fund would be adequate to clean up the site when the plant ceases operation. The guarantee was issued after the NRC expressed concern that there was not enough money in the trust to fund the site's cleanup.

Source: http://www.reformer.com/localnews/ci_15074432

8. *May 13, WMBF 32 Myrtle Beach* – (South Carolina) **Nuclear plant makes changes after fires.** Workers at the H.B. Robinson Nuclear Plant in Hartsville, South Carolina said they are making changes after two fires forced the plant to shut down in March. A spokesperson for Progress Energy said May 12 the company presented findings of an internal investigation into what happened to the Nuclear Regulatory Commission. The month-long investigation involving 20 people from the company revealed a fuse in one-of-five 4,000 volt electrical panels caused a fire. Officials said the fuse then started a second fire a short time later. Safety systems managed to keep the fire under control, allowing employees to extinguish it within 10 minutes. The spokesperson for Progress

Energy added the plant is making 31 changes to prevent the problem from happening again. “All of our safety systems worked as they are designed to work,” he explained. Officials state the changes range from more training for workers to new equipment being installed. Now the company waits for the NRC to release its findings.

Source: <http://www.wmbfnews.com/Global/story.asp?S=12479951>

9. *May 13, Associated Press* – (Maryland) **Calvert Cliffs reactor shuts down.** A spokesman for the Calvert Cliffs nuclear power plant says one of its two reactors has shut down automatically after the unit’s link to the regional power grid apparently failed. The reactor at the Southern Maryland nuclear plant shut down shortly before 2 p.m. May 12. The incident was under investigation, and it was not known how long it would take to bring the unit back online. The reactor normally provides about 10 percent of the state’s electricity.

Source: <http://voices.washingtonpost.com/local-breaking-news/nuclear-reactor-in-md-shuts-do.html>

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

Critical Manufacturing Sector

10. *May 14, IDG News Service* – (National) **Car hackers can kill brakes, engine, and more.** University researchers have taken a close look at the computer systems used to run today’s cars and discovered new ways to hack into them, sometimes with frightening results. The security researchers said that by connecting to a standard diagnostic computer port included in late-model cars, they were able to do some nasty things, such as turning off the brakes, changing the speedometer reading, blasting hot air or music on the radio, and locking passengers in the car. In a late 2009 demonstration at a decommissioned airfield in Blaine, Washington, they hacked into a test car’s electronic braking system and prevented a test driver from braking a moving car — no matter how hard he pressed on the brakes. In other tests, they were able to kill the engine, falsify the speedometer reading, and automatically lock the car’s brakes unevenly, a maneuver that could destabilize the car traveling at high speeds. They ran their test by plugging a laptop into the car’s diagnostic system and then controlling the car’s computer wirelessly, from a laptop in a vehicle riding next to the car.

Source:

http://www.computerworld.com/s/article/9176778/Car_hackers_can_kill_brakes_engine_and_more

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

Defense Industrial Base Sector

11. *May 13, Associated Press* – (California) **Mules will help in radiation survey at LA-area lab.** The Environmental Protection Agency has a new weapon in the fight against radioactive contamination at a Los Angeles-area lab: Mules. The EPA will use four mules to carry high-tech scanning equipment to detect radiation on steep and rocky

terrain at the Santa Susana Field Laboratory. The EPA is conducting a survey of soil and water contamination at the lab near Simi Valley, where rocket engines were tested for years and a partial meltdown of a nuclear reactor took place in 1959. About 500 acres of the lab will be scanned for gamma radiation. Results will be turned over to the state, which is overseeing the cleanup.

Source:

http://www.google.com/hostednews/ap/article/ALeqM5iilMOu_kxQdP7sexHnQuyuuVfoxwD9FM1ALO0

12. *May 12, Aviation Week* – (Florida) **Shuttle program prepares to shut down.** The shuttle Atlantis is poised for its final scheduled mission — the delivery of a compact Russian docking and laboratory module to the International Space Station. Liftoff from Kennedy Space Center is set for May 14 at 2:20 p.m. The spacecraft's six-man crew has trained to deliver *Rassvet*, or "Dawn," a 23-ft.-long compartment that will open a fourth docking port on the orbiting lab for the Russian Soyuz and Progress capsules, which will continue to come and go long after Atlantis, and then orbiters Discovery and finally Endeavour, complete their final flights by year-end. Last week, in a harbinger of things to come as the program winds down, shuttle contractors shed 800 workers from hardware production, launch and landing support, as well as the spare-parts depot, shrinking the national shuttle workforce to 10,700, according to the NASA shuttle program manager. Once Atlantis returns to Earth, only two scheduled missions remain, with officials still angling to pin down the departure dates.

Source:

http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=space&id=news/awst/2010/05/10/AW_05_10_2010_p43-224530.xml

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

Banking and Finance Sector

13. *May 14, Indo-Asian News Service* – (International) **Explosions rock Bangkok's financial district.** Six explosions rocked the Bangkok, Thailand financial district May 14, as troops and protesters clashed to control the heart of the capital. Unknown assailants fired M79 grenades at soldiers stationed at the Saladaeng skytrain station on Silom Road, the main financial district and a popular entertainment area, Thai media reports said. Residents in the neighborhood said they heard six explosions. Two people were wounded, according to The Nation newspaper's Web site. The grenade attacks coincided with a military offensive against anti-government protesters who have blockaded themselves in an area around Ratchaprasong Road, a posh commercial district, just north of Silom. At least one demonstrator was killed May 14, and eight protesters and two journalists were hurt in the latest unrest, which took place after the Thai government launched an offensive the night before to drive thousands of followers of the United Front for Democracy Against Dictatorship (UDD) from Ratchaprasong.

Source: <http://www.hindustantimes.com/Explosions-rock-Bangkok-s-financial-district/Article1-543668.aspx>

See item [40](#)

14. *May 14, Associated Press* – (International) **Underground broker network a bane in terror probes.** Long before there was MoneyGram and Western Union, people in South Asian countries often used an informal network of brokers, called an “hawala,” to transfer money over long distances when it was too inconvenient or dangerous to send cash by courier. Today, the centuries-old system still exists and is used to move billions of dollars annually in and out of countries like Pakistan, Afghanistan, and Somalia — often to the chagrin of U.S. law enforcement. A federal law enforcement official told The Associated Press that a terror suspect is believed to have tapped into such a network to help fund a plot to detonate a car bomb in Times Square May 1. The official spoke on condition of anonymity because the investigation is ongoing. Authorities said three Pakistani men — two in the Boston area and one in Maine — supplied funds to the suspect but may not have known how the money would be spent. The three have been arrested on immigration violations. While most money transfers made through these hawaladars, or brokers, are benign, the system is also routinely used by drug smugglers, terrorists, and other criminals who want to move money without leaving a paper trail.
Source: <http://www.google.com/hostednews/ap/article/ALeqM5iAVtGRdd1bq4oG0wjEyF-Iqq6Y5wD9FMKM301>
15. *May 14, Hartford Courant* – (National) **Feds close in on network of high-tech ATM thieves.** A federal task force continued to close in May 13 on a high-tech network of Romanian thieves who are using electronic spyware to loot the accounts of ATM customers at banks in Connecticut and elsewhere in the Northeast. Federal prosecutors disclosed that they have indicted four more Romanian nationals in the scheme, which has resulted in hundreds of thousands of dollars in losses. The task force of federal, state and local police agencies charged another two suspects one year ago, and it is continuing to hunt for other suspects. All those charged so far in the scheme are accused of installing what are known as skimming devices on ATM machines and on card-activated door locks that banks use to control access to the machines. In addition, the suspects in the scheme are accused of installing pinhole cameras on ATM machines. Banks, which credit customer accounts for fraudulent withdrawals, are the ultimate victims of the scheme, according to federal prosecutors. A U.S. Attorney said May 13 that the four Romanian nationals named in the indictment emptied accounts in Connecticut, New York and Pennsylvania. The four are being held without bail, authorities said.
Source: <http://www.courant.com/news/connecticut/hc-hc-atm-skim-0514.artmay14,0,757871.story>
16. *May 14, MetroWest Daily News* – (Massachusetts) **Suspicious package in Natick is cooler.** A suspicious package found in a parking garage beneath a Summer Street building in Natick, Massachusetts, May 13 turned out to be a cooler containing two ice packs, police said. The Middlesex Savings Bank’s Operations Center at 37 Summer Street was evacuated after an employee discovered the package in an underground parking lot at 8:37 a.m., a police spokesman said. Police also blocked off portions of Summer Street as a precaution. The police and fire departments went to the building.

The spokesman said he and another police lieutenant went into the parking garage and found the package, a Styrofoam cooler with the top taped down. Because there had been no threats and no reports of disgruntled employees, the two officers decided to open the lid and discovered two spent ice packs.

Source: <http://www.metrowestdailynews.com/news/x1773731849/Suspicious-package-in-Natick-is-cooler>

17. *May 13, DarkReading* – (International) **Authorities arrest first suspect in massive identity-theft ring.** Indian police said May 12 that they have detained a Ukrainian man charged in the U.S. with stealing some 40 million credit and debit card numbers. The suspect was detained after he landed in New Delhi on a domestic flight from the southwestern holiday state of Goa May 10, a police spokesman said. He is one of 11 people wanted by the U.S. Justice Department in “the largest hacking and identity theft case ever prosecuted,” which was filed in August 2008. Besides the suspect, three Americans, two Ukrainians, two Chinese, one Estonian, a Belarussian and an unidentified suspect are on the wanted list, the Justice Department said. The group is accused of obtaining credit and debit card numbers by hacking into the computer networks of major U.S. retailers — including Barnes & Noble, OfficeMax, shoe retailer DSW, and Sports Authority. Once inside the network, “sniffer programs” captured credit card numbers, passwords, and account information, police said. The data was stored in encrypted servers controlled from Eastern Europe and the United States.

Source:

http://www.darkreading.com/database_security/security/cybercrime/showArticle.jhtml?articleID=224701874

18. *May 13, St. Paul Pioneer Press* – (National) **Banks may be tapped for Ponzi victims.** With \$3.5 billion in losses, Petters Co. Inc., a Minnetonka-based Ponzi scheme, was one of the largest the U.S. has seen. But it was not unique. Dozens of other smaller schemes have deflated in recent years, and some attorneys are looking at new ways to get money for victims. Their target: the banks that handled the big inflows and outflows of cash. A former federal prosecutor and attorney with the U.S. Securities and Exchange Commission has four civil cases pending against banks where Ponzi schemers had their accounts. He argues the banks aided the scams that bilked people out of millions of dollars. They knew — or should have known — what was really going on. The former federal prosecutor is seeking judgments against Bank of America in three of the cases and JP Morgan Chase in the fourth. Those cases are still moving through the courts and have not been resolved.

Source: http://www.twincities.com/business/ci_15082383

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

Transportation Sector

19. *May 14, WISC 50 Madison* – (Wisconsin) **Bomb squad called to investigate semitrailer.** Authorities in Wisconsin were continuing to investigate after the driver of a semitrailer truck led police on a pursuit through Monroe County May 13. The

Wisconsin State Patrol said the truck was eventually stopped using tire spikes after a nearly 30-minute chase. When the driver refused to get out of the truck for more than an hour, he emerged with a unidentified package. The driver was shot with non-lethal rounds and was being evaluated at a hospital, officials said. Amid initial concerns about the truck's cargo, authorities said that no explosives or contraband of any kind were found inside the truck May 14. The Monroe County sheriff said that an hours-long search resulted in authorities finding only the truck's load of energy drinks.

Source: <http://www.channel3000.com/news/23549139/detail.html>

20. *May 13, WTOP 1500 Washington* – (Maryland) **Metro: No safety hazard in near-miss on Red Line.** The Washington Metropolitan Area Transit Authority (Metro) said there was no safety hazard last week when a Red Line train operator hit the emergency brake because he felt he was getting too close to another train. According to a Metro report on the incident released May 13, the trains stopped 600 feet apart from one another near the Wheaton station May 5. But the head of the Tri-State Oversight Committee told WTOP the trains were too close for comfort. There were passengers on both trains at the time. No one was injured. Metro said the passengers were not in any danger at the time. The incident was not immediately reported. Safety personnel started their investigation the day after the incident — a move Metro officials said was “unacceptable.” Metro also did not notify the Tri-State Oversight Committee within the required two-hour time frame.

Source: <http://wtop.com/?nid=25&sid=1956606>

21. *May 13, U.S. Department of Homeland Security* – (National) **Secretary Napolitano announces nearly \$790 million in Critical Infrastructure and Preparedness Grants.** The Homeland Security Secretary on May 13 announced the fiscal year 2010 Preparedness Grants for nine federal programs, totaling nearly \$790 million to assist state, local, and tribal governments and the private sector in strengthening preparedness for acts of terrorism, major disasters, and other emergencies. The FY 2010 grants announced include the following programs: Transit Security Grant Program, Freight Rail Security Grant Program, Intercity Passenger Rail (Amtrak), Intercity Bus Security Grant Program, Port Security Grant Program, Buffer Zone Protection Program, Emergency Operations Centers Grant Program, Interoperable Emergency Communications Grant Program, and Driver's License Security Grant Program.

Source: http://www.dhs.gov/ynews/releases/pr_1273760215810.shtm

22. *May 13, New York Post* – (International) **Kennedy passenger flies to Cairo with guns and swords.** An EgyptAir passenger flew from Kennedy Airport to Cairo with a mini-arsenal of two pistols, 250 rounds of ammo, two swords and 11 daggers in his checked bags — right under the noses of JFK security monitors. The man, whose age and address were not given, was arrested after he arrived in Cairo yesterday, Egyptian media said. The man was identified as a botany professor at a U.S. college. He was detained after his weapons cache was discovered during a routine inspection at the Cairo airport, authorities said. It was unclear what Egyptian laws the man is accused of violating. But he failed to declare the weapons to EgyptAir, the Transportation Security Administration (TSA) reported. His weapons cache would have been allowed under

U.S. law, so long as it was in his checked luggage and properly declared to the airline, the TSA said. EgyptAir's rules allowed him to carry two pistols and 10 pounds of ammo in checked baggage, so long as he declared them. U.S. airlines have similar rules, and the TSA requires weapons to be stowed in locked, hard-sided containers.

Source:

http://www.nypost.com/p/news/local/queens/jfk_passenger_sneaks_guns_aboard_096NR5juBOcwb8YbTGIO9H

23. *May 13, USA TODAY* – (National) **FAA to fine Continental \$325,000 for landing gear problem.** The Federal Aviation Administration (FAA) has proposed fining Continental \$325,000 for a safety violation. That move continues what appears to be stepped-up regulatory enforcement effort by the agency. As for the fine, the FAA alleges Continental operated a Boeing 737 on a dozen or more flights without fixing a possible problem with its landing gear. The Associated Press details the FAA's allegation, writing: "The crew of a Continental Boeing 737 flying from Houston to Los Angeles in December 2008 saw a warning light related to the plane's right main landing gear, but decided after discussing the problem with the airline's maintenance department to continue the flight, the FAA said. After takeoff, the flight wound up being diverted to Phoenix after the crew noticed the plane was burning excessive fuel. On the ground, Continental maintenance workers inspected the landing gear but did not make a required entry in the plane's maintenance log or any other maintenance record about the abnormal landing gear indication, FAA said." In total, the FAA said the Continental 737 flew at least 12 additional passenger flights before the problem was addressed, according to AP. Continental officials did not immediately respond to AP's request for a comment.

Source: <http://www.usatoday.com/travel/flights/item.aspx?type=blog&ak=92481.blog>

24. *May 13, KRQE 13 Albuquerque* – (New Mexico) **Human remains leak blood in cargo hold.** Baggage handlers at Albuquerque International Sunport got a nasty surprise when they opened up the cargo hold on Southwest Flight 477 May 12. Blood from human remains being transported on the flight managed to leak out of the shipment container. "A few agents that were working that flight," a source with knowledge of the incident said, "said they wouldn't offload that flight because they said there was blood everywhere." Sources said that the blood got onto the clothes of several workers and that it leaked onto some of the passengers' luggage. Southwest employees want to know how this could happen and if the airline took enough precautions cleaning up the mess. An airport spokesperson, airport police, and the airport director at Sunport all told News 13 they were not contacted by Southwest yesterday regarding any sort of potential biohazardous leak. Authorities said airlines are not required to contact authorities about these types of situations unless a haz-mat crew is needed.

Source: <http://www.krqe.com/dpp/news/local/central/human-remains-leak-blood-in-cargo-hold>

For more stories, see items [5](#) and [59](#)

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

Postal and Shipping Sector

Nothing to report

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

Agriculture and Food Sector

25. *May 14, Food Safety News* – (National) **CDC issues update on E. coli O145 outbreak.** On May 13, the Centers for Disease Control and Prevention (CDC) issued an update on the E. coli O145 outbreak linked to Freshway Foods romaine lettuce. As of May 11, there are 23 confirmed and 7 probable cases related to this outbreak from Michigan, New York, Ohio, and Tennessee. The number of ill persons identified in each state with this strain is: Michigan (10 confirmed and 3 probable), New York (4 confirmed and 3 probable), Ohio (8 confirmed and 1 probable), and Tennessee (1 confirmed). To diagram the outbreak trend, the CDC has created an epidemic curve, or a chart that describes the number of persons that became ill each day. Among the confirmed and probable cases with reported dates available, illnesses began between April 10 and April 26. Infected individuals range in age from 13 years old to 31 years old and the median age is 19 years. Sixty-six percent of patients are male. Health investigators in New York recently obtained an E. coli O145 isolate from an unopened bag of romaine lettuce that matches the outbreak strain. A separate case-control study in Michigan supported this, finding a significant association between illness and consumption of romaine lettuce from the same processing facility, which is believed to be located in Yuma, Arizona. The CDC said that investigators are using pulsed-field gel electrophoresis, a type of DNA fingerprint analysis of E. coli bacteria obtained through diagnostic testing to identify cases of illness that might be part of this outbreak. This testing is done in public health laboratories as part of the PulseNet network. Investigators have established a common definition of confirmed and probable cases related to this outbreak. An Ohio resident filed an E. coli lawsuit against Freshway Foods May 11.

Source: <http://www.foodsafetynews.com/2010/05/update-in-e-coli-o145-outbreak/>

26. *May 13, Food Poison Journal* – (National) **Pumpkin butter and sweet potato butter recalled for botulism.** It was announced today that Amish Wedding Foods, Inc. of Ohio, is recalling all lots of 9-, 16-, and 18-ounce pumpkin butter, and 16- and 18-ounce sweet potato butter due to possible botulism contamination. Thus far no illness have been reported. The pumpkin and sweet potato butters were sold around the U.S. under a variety of brand names.

Source: <http://www.foodpoisonjournal.com/2010/05/articles/food-poisoning-watch/pumpkin-butter-and-sweet-potato-butter-recalled-for-botulism/>

27. *May 13, Bloomberg* – (International) **Miyazaki plans to slaughter 80,000 pigs, cows on foot-and-mouth outbreak.** Japan plans to slaughter more than 80,000 livestock in

the southern prefecture of Miyazaki as it seeks to contain an outbreak of foot-and-mouth disease. A total of 73,653 pigs and 6,604 cows have been marked for destruction at 86 farms, the Miyazaki local government said in a statement yesterday. Japan's farm minister said the government plans to compensate farmers, the Nikkei newspaper reported.

Source: <http://preview.bloomberg.com/news/2010-05-13/miyazaki-plans-to-slaughter-80-000-pigs-cows-on-foot-and-mouth-outbreak.html>

28. *May 13, Miami Herald* – (Florida) **Court upholds \$11M citrus canker payout, but Florida vows to appeal.** For Broward Countians who sued the Florida Department of Agriculture over its controversial citrus canker-eradication program, an appellate court victory May 12 was as bittersweet as an unripe Honeybell. The Fourth District Court of Appeal unanimously held that some 55,000 Broward property owners are due \$11 million for healthy trees felled by state chainsaws from 1995 to 2006. "Government has regulatory power for the very purpose of safeguarding the rights of citizens, not for destroying them," the judges wrote. "Under any possible meaning, if government cuts down and burns private property having value, then government has taken it. And if government has taken it, government must pay for it." Confirming a widely held belief among property owners, the ruling said it was "apparent from the history of this case that [the Department] destroyed these privately owned healthy trees not because they were 'imminently dangerous' to anybody, but instead to benefit the citrus industry." The decision upholds a 2008 Broward jury verdict, but it won't end the long-running case. "We respectfully disagree with the appeal court, and we will appeal it to the Florida Supreme Court," a Florida Department of Agriculture spokesman said, citing \$44.5 million already paid on claims around the state. Although the decision applies only to the Broward suit, a plaintiffs' attorney said it will affect class actions pending in Miami-Dade, Palm Beach, Lee and Orange counties. The eradication program began after agriculture officials discovered a diseased tree near Miami International Airport. Source: <http://www.miamiherald.com/2010/05/12/v-fullstory/1626774/citrus-canker-windfall-hits-a.html>
29. *May 13, Geneva Sun* – (Illinois) **Two hurt in Geneva factory blast.** Fire investigators continue to seek the source and cause of an explosion that injured two workers May 12 at a food-flavoring factory in Geneva, Illinois. One employee of the FONA International plant was taken by ambulance to Delnor Community Hospital, a Geneva Fire Department lieutenant said. Another worker was treated at the scene before being sent home, he said. The blast occurred about 9:15 p.m. in the factory at 1900 Averill Road. It is on the campus of an industrial park located northeast of Roosevelt and Kirk roads. The lieutenant said the explosion occurred during "a manufacturing process, and was confined to a room inside the building." He did not know how many employees were on duty at the time. Twenty Geneva firefighters were sent to the scene, along with a contingent from the St. Charles Fire Department, the lieutenant said. No firefighters were hurt during the incident, and rescuers left the scene about 10:36 p.m., he said. FONA International makes food flavorings, according to the company's Web site. Its 82,000-square-foot plant and corporate headquarters employed 174 people in 2009.

Source: http://www.suburbanchicagonews.com/genevasun/news/2268762,Geneva-factory-blast_AU051210.article

30. *May 13, Associated Press* – (Louisiana) **State closes 1 oyster harvesting area, reopens 2.** The Louisiana Department of Health and Hospitals (DHH) has closed another harvesting area in response to the oil spill in the Gulf of Mexico, while two others were scheduled to reopened at sunrise May 14. The DHH Secretary said Area 17, west of the Mississippi River in Terrebonne Parish, closed at sundown May 13. He said areas 9 and 13, however, were reopened to give harvesters as much time as possible to bring in their product before any potential impact from the spill. Area 9 is in Plaquemines Parish and Area 13 covers Lafourche and Jefferson parishes. DHH said oil has not reached those locations, noting they are still being monitored daily. In addition, harvesters are tasting oysters pulled from the waters to make sure the product is good. Source: <http://www.wdam.com/Global/story.asp?S=12480539>
31. *May 12, FDA & Baroody Imports, Inc.* – (New Jersey; New York) **Baroody Imports, Inc. issues allergy alert on undeclared sulfites in Baroody dried apricots.** Baroody Imports, Inc., a Clifton, New Jersey firm, is recalling Baroody Dried Apricots because it may contain undeclared sulfites. People who have severe sensitivity to sulfites run the risk of serious or life-threatening allergic reactions if they consume this product. The recalled 14.1 oz/400 gr. packages of dried apricots were sold in New Jersey and New York. The recall was initiated after routine sampling by New York State Department of Agriculture and Markets Food Inspectors revealed the presence of undeclared sulfites in packages which did not declare sulfites on the label. The consumption of 10 milligrams of sulfites per serving has been reported to elicit severe reactions in some asthmatics. Anaphylactic shock could occur in certain sulfite sensitive individuals upon ingesting 10 milligrams or more of sulfites. No illnesses have been reported to date in connection with this problem. Source: <http://www.fda.gov/Safety/Recalls/ucm212092.htm>
32. *May 12, Associated Press* – (North Dakota) **Horace, ND plant evacuated after fire breaks out.** The SunGold Foods plant in the Cass County town of Horace, North Dakota was evacuated as a precaution after a fire broke out in an oven roasting sunflower seeds. The Cass County sheriff's office said the seeds caught on fire about 1:40 p.m. May 12, and flames spread to the oven's exhaust, which fell down and ignited other items. A sheriff's deputy said that about 20 workers gathered outside the plant. He said no one was injured. A damage estimate was not immediately available. Source: <http://www.wday.com/event/article/id/33431/>

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

Water Sector

33. *May 13, WSMV 4 Nashville* – (Tennessee) **Repairs, tests continue on damaged water plant.** A Nashville, Tennessee water plant that was damaged by severe flooding earlier this month could be in operation in a few weeks, but that is not prompting an

end to water conservation measures. Officials said high water destroyed the electrical and computer systems at the Donelson's K.R. Harrington Water Plant, flooded pumps and motors and contaminated basins and storage wells at the facility. Every electrical outlet will have to be replaced. The chemical feed system will be tested, and similar to how a pool filter is backwashed, every water filter will have to be flushed. Clear wells, which hold water underground, have been drained and will be thoroughly cleaned. Once all that is complete, samples will be sent to a lab. But this progress does not mean water levels have returned to normal. "I believe our residents and businesses should be prepared to continue with their conservation efforts at least through the end of this month, through the end of May," said the Nashville mayor. City leaders said water reserves are at 90 percent, but until the Harrington plant is working again, Metro Water customers are asked to conserve. Non-essential water use, such as washing cars, is still prohibited. The mayor revised the conservation requirements May 13, suggesting Nashvillians can now start using about 70 percent of their normal water use.

Source: <http://www.wsmv.com/weather/23539796/detail.html>

34. *May 13, News 8 Austin* – (Texas) **Reward offered for information on vandalized wastewater line.** The Austin Water Utility (AWU) in Austin, Texas hopes to get a sewage spill cleaned up and add a layer of topsoil to the source before rain expected for May 14 brings the potential for both waste and bacteria to spread. On May 9, someone vandalized a wastewater line by dumping construction debris into it. That created a 250,000-gallon sewage spill. Much of the spill polluted a creek that feeds the Barton Springs portion of the Edwards Aquifer. Private well users who live in the area surrounded by Mopac, Manchaca Road, the Shady Hollow neighborhood, and Barton Springs Road are being asked to boil drinking water for two minutes before consuming it. Now, AWU is raising awareness and raising the stakes for finding who clogged the waste-water line with debris. The agency is offering a \$5,000 reward for information leading to an arrest and conviction. Crimestoppers is offering an additional \$1,000. The Austin Police Department said they believe a truck may have carried the debris to the manhole. They also believe the crime was planned out because the manhole cover is bolted down and weighs between 60 and 70 pounds. "I don't believe one man could have done it," an Austin Police Department detective said. "They would have had to have brought tools, so there was some forethought into what was done." The incident is currently considered criminal mischief, but circumstances could change as the environmental impact is further observed and more agencies get involved. The cleanup could easily exceed \$20,000, which classifies it as a third degree felony.

Source: <http://news8austin.com/content/headlines/270992/reward-offered-for-information-on-vandalized-wastewater-line>

35. *May 13, United States Department of Justice* – (New York) **City of Oswego, N.Y., agrees to invest \$87 million in upgrades to sewer system.** To resolve long-standing problems with unpermitted sewer overflows, the city of Oswego, New York, will invest an estimated \$87 million in improvements to its west side sewer system, the Justice Department and U.S. Environmental Protection Agency (EPA) announced May 13. The improvements to the city's sewer system, to be implemented under the settlement lodged in federal court in Syracuse, New York, will significantly reduce the number of

sewer overflows. The city also will pay a penalty of \$99,000. The settlement resolves claims against the city by both the United States and the state of New York. Under the settlement, the city has agreed to undertake a comprehensive, system-wide program that will bring the city into compliance with the Clean Water Act. Specific improvements include: requiring at least 75 percent separation of the combined system into sanitary and stormwater components, in order to prevent high volumes of rainwater from overwhelming the treatment plant; expanding the west side wastewater treatment plant's treatment capacity by 50 percent; disconnecting catch basins to reduce the inflow of rainwater into the existing sanitary sewer system; undertaking major improvements to the operation and maintenance program; and implementing sewer financing reforms.

Source: <http://www.justice.gov/opa/pr/2010/May/10-enrd-562.html>

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

Public Health and Healthcare Sector

36. *May 14, Des Moines Register* – (Iowa) **Grundy Center hospital evacuated after gas-leak scare.** Patients were evacuated for about two hours May 12, after a gas-leak scare at Grundy County Memorial Hospital in Grundy Center, Iowa. A gas odor filled the hospital about 3:30 p.m. Patients were taken from the older part of the hospital into a medical building that's under construction. One patient was transferred to Allen Hospital in Waterloo. Workers doing some landscaping in a new healing garden hit an old gas pipe. Officials said the old pipe was gas-free.

Source: <http://www.desmoinesregister.com/article/20100514/NEWS/5140358/-1/PROM/Grundy-Center-hospital-evacuated-after-gas-leak-scare>

37. *May 13, Chicago Sun-Times* – (Missouri) **Hazmat called to Saint Elizabeth Hospital.** A haz-mat team responded the scene of a compressed oxygen leak at Saint Elizabeth Hospital in Chicago, May 13. The precautionary call indicated a possible leak from a compressed oxygen tank in the parking lot of Saint Elizabeth Hospital. No injuries have been reported and no buildings were evacuated.

Source: <http://cbs2chicago.com/local/hazmat.hospital.oxygen.2.1692807.html>

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

Government Facilities Sector

38. *May 14, Mid Columbia Tri-City Herald* – (Washington) **Work stops for safety evaluation at Hanford plant.** Work was stopped May 13 at the Hanford Plutonium Finishing Plant in Hanford, Washington for a safety standdown after a worker cut or scraped himself on debris that possibly was radiologically contaminated. CH2M Hill Plateau Remediation Co. management was concerned that safety-related procedures were not rigorously being followed in recent weeks and voluntarily called a halt to most work with radiological materials at the plant, said a company spokeswoman. In addition, a worker in late March inhaled nitric acid fumes that apparently dripped on

his respirator as a liquid chemical feed line was being removed. That and concerns about an earlier ventilation system incident at the plant caused a site representative for the Defense Nuclear Facilities Safety Board to speculate in early April that the incidents might be leading indicators of a more serious problem. “We know that we need to do some critical self-assessment,” the spokeswoman said. “We know there are some issues that need work.” The Department of Energy (DOE) contractor chose to stop work as a conservative approach to safety issues rather than at DOE’s direction. Source: <http://www.tri-cityherald.com/2010/05/14/1013908/work-stops-for-safety-evaluation.html>

39. *May 14, Lansing State Journal* – (Michigan) **Protesters arrested in Lansing for trespassing at the Capitol.** Michigan State Police troopers and security officers arrested 13 adults and apprehended one juvenile for trespassing Wednesday night, May 12, when they refused to leave the State Capitol after it closed. Representing By Any Means Necessary, a civil rights group, those arrested and apprehended had been protesting an academic plan for Detroit schools when the Capitol’s facilities manager apparently asked the demonstrators to leave and they refused, according to state troopers. “We want to ensure everyone is allowed to exercise their constitutional rights, but when violations of the law occur, we are obligated to take enforcement action,” said a spokesman with the state police Lansing post. “We gave the demonstrators every opportunity to leave on their own prior to being charged with trespassing, including as they were being taken into police custody.” According to troopers, the adults are in custody at the Lansing City Jail, pending posting of \$250 bonds or arraignment. All were from the Detroit area.

Source:

<http://www.lansingstatejournal.com/article/20100513/NEWS01/305130005/1002/NEWS01/Protesters-arrested-in-Lansing-for-trespassing-at-the-Michigan-State-Capitol>

40. *May 14, Associated Press* – (International) **Thai troops fire at rioting protesters.** Thai troops fired bullets at anti-government protesters, and explosions thundered in the heart of Bangkok, Thailand, Friday, May 14 as an army push to clear the streets and end a two-month political standoff sparked clashes that have killed eight and wounded 101. As night fell, booming explosions and the sound of gunfire rattled around major intersections in the central business district. Local TV reported that several grenades hit a shopping center and elevated-rail station. Plumes of black smoke hung over the neighborhood as tires burned in eerily empty streets while onlookers ducked for cover. With security deteriorating and hopes of a peaceful resolution to the standoff increasingly unlikely, what was once one of Southeast Asia’s most stable democracies and magnets of foreign investment has been thrust deep into political uncertainty. The crisis threatens its stability, economy and already-decimated tourism industry. Friday’s violence was initially centered on a small area home to several foreign embassies, including those of the U.S. and Japan which were forced to close. But by midafternoon, the violence had spread around the 1-square-mile (3-square-kilometer) protest zone barricaded with bamboo stakes and tires. The British, New Zealand and the Dutch embassies, which are in the vicinity, also were shut.

Source: http://www.google.com/hostednews/ap/article/ALeqM5g3j-vAVG1fg3kEfnogTiH8_4EXvwD9FMN0AG0

See item [13](#)

41. *May 13, WIS 10 Columbia* – (South Carolina) **Unstable, explosive chemicals removed from Voorhees College.** A hazardous materials team had to remove 18 canisters of an explosive chemical from Voorhees College, Denmark South Carolina Fire Department officials said May 13. “It’s flammable, highly flammable, that’s what’s scary about ether,” a National Environmental Management Service worker said about diethyl ether. “It’s more flammable than gasoline.” On Thursday, the worker neutralized 18 canisters full of the chemical at Voorhees College. He said the chemical has a one-year shelf life. The state department of health and environmental control believes the canisters full of the chemical were 25 years old. “Over time it forms peroxides which are very unstable,” said the worker. “Just turning the cap could cause it to explode.” The worker specializes in removing dangerous chemicals from college campuses. It only took him an hour to complete his work at Voorhees. “We prepared big and luckily it was smaller than what we thought,” said a fire chief.

Source: <http://www.wistv.com/Global/story.asp?S=12476362>

42. *May 13, The Telegraph* – (Illinois) **Bomb threats found at two schools.** Two Alton, Illinois district schools were targets of bomb threats May 13, forcing evacuation of students and building searches, with authorities finding no explosives. The disruptions taxed school officials and local law-enforcement agencies. The first bomb threat, in the morning at North Elementary School, 5600 Godfrey Road, in Godfrey, forced students to be bused temporarily to Lewis and Clark Community College. The second threat, in the afternoon at the main building at Alton Middle School, forced relocation of about 750 students — roughly half the student body — and tied up traffic on its Pit parking lot and in the 2200 block of College Avenue. “We took it seriously, but there was not any substance to it,” the Alton police chief said about the threat at Alton Middle School. “It’s sad that they keep resorting to this horseplay. It disrupts the learning environment, and it is a drain on city resources.” The chief said 18 Alton officers responded to the school. Police did not use a canine for the search. “It took nine officers to secure the main building, and nine on the perimeter for traffic control and the evacuation,” he said. That left only two officers to respond to any other calls in the city for more than an hour.

Source: <http://www.thetelegraph.com/news/alton-40075-police-school.html>

43. *May 13, Bellingham Herald* – (Oregon) **DEPOT: Mustard weapon agent vapor detected.** Trace amounts of mustard chemical agent vapor were detected May inside a storage igloo at the Umatilla Chemical Depot in Umatilla, Oregon. There was no danger to the public or the environment, according to the depot. The igloos have a passive filtration system that prevents chemical-agent vapor from escaping the structure. Officials said the leaking container would be identified and repaired.

Source: <http://www.bellinghamherald.com/2010/05/13/1430077/depot-mustard-weapon-agent-vapor.html>

44. *May 13, Nextgov* – (National) **Laptop stolen from VA contractor contains veterans' personal data.** A laptop belonging to a contractor working for the Veterans Affairs Department (VA) was stolen earlier this year and the personal data on hundreds of veterans stored on the computer was not encrypted, a violation of a VA information-technology policy, said the top-ranking Republican on the House Veterans Affairs Committee. The VA reported the theft of the laptop from an unidentified contractor to the committee April 28, and informed members that the computer contained personally identifiable information on 644 veterans, including data from some VA medical centers' records, according to a letter to the VA Secretary sent by a Republican Congressman from Indiana. The data was not encrypted, which would have prevented a thief from accessing the information, a requirement Congress and VA issued to all department contractors in 2006 after a laptop containing health data on more than 26 million veterans and their spouses was stolen from a VA employee's home. That laptop later was recovered. The laptop in the recent theft was stolen from a contractor employee's car April 22, and she notified local police within 10 minutes, the chief information officer at VA said. Although the vendor had certified to VA that it had encrypted laptops that stored department data, the chief information officer confirmed the data on the stolen laptop was unencrypted.

Source: http://www.nextgov.com/nextgov/ng_20100513_1937.php?oref=topstory

45. *May 13, WFTV 9 Orlando* – (Florida) **Teen arrested for bomb threats at school.** A Brevard County teenager is facing charges for allegedly making bomb threats at his Palm Bay, Florida school. Police arrested the 16-year-old, May 12. Detectives said he wrote several notes threatening to blow up Southwest Middle School. Another student found one of the notes in a classroom. Police said the student admitted to writing the notes, which included threats about his parents.

Source: <http://www.wftv.com/news/23539589/detail.html>

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

Emergency Services Sector

46. *May 13, KPTV 12 Portland* – (Oregon) **Vandals break windows at police substation.** Several large windows were broken at a police substation in north Portland, Oregon between May 12 and 13. The small office on North Denver Street, which serves the Kenton neighborhood, was closed at the time of the vandalism. Neighbors said the windows were boarded up when they first saw the building early on the morning of May 13. A Portland police spokeswoman said officers are investigating.

Source: <http://www.kptv.com/news/23546380/detail.html>

47. *May 12, WLBT 3 Jackson* – (Mississippi) **Fire evacuates Madison County Jail.** Inmates housed at the Madison County Jail in Canton, Mississippi had to be evacuated May 12. A maintenance crew was installing a new air-conditioning unit on the roof when hot metal sparked a fire between the roof and the ceiling. All 144 inmates in the building were moved to safety as it filled with smoke. No one was injured. "It couldn't have happened at a better time, if it had to happen, because it was

right at shift change. We had a lot of detention officers in the jail. They were able to move all the inmates out into the yard, which is our fire protocol. We called in every man we have,” said the chief deputy. Deputies said the smoke and water would be cleaned up in time for the inmates to be back in their cells the night of May 12.

Source: <http://www.wlbt.com/Global/story.asp?S=12471111>

For another story, see item [21](#)

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

Information Technology Sector

48. *May 14, V3.co.uk* – (International) **Twitter phishing scam uses iPhone 4G bait.** Security experts are warning of a Twitter phishing scam designed to harvest personal data with the offer of a new iPhone 4G as a lure. A Sophos senior technology consultant wrote in a blog post that the scam employs a “gaggle of profiles, using avatars of sexy young women, pumping out messages to users” saying they could win the device. “A quick look at one of the Twitter accounts spamming out the messages underlines that she is by no means a regular user, but set up specifically to advertise a data-collecting form on behalf of the shady guys behind this scheme,” he said. “Clicking on any of these links takes you to a Web page (currently offering an iPod Shuffle as a prize, rather than an iPhone 4G - that’s a letdown, isn’t it?) that asks you to fill in a form with your personal data.” The form asks users to fill in information such as date of birth, marital status, telephone number and address.
Source: <http://www.v3.co.uk/v3/news/2263048/phishing-spam-spotted-iphone-4g>

49. *May 13, The Register* – (International) **Twitter-controlled botnets come to the unwashed masses.** A security researcher has unearthed a tool that simplifies the process of building bot armies that take their marching orders from specially created Twitter accounts. TwitterNet Builder offers script kiddies a point-type-and-click interface that forces infected PCs to take commands from a Twitter account under the control of attackers. Bot herders can then force the zombies to carry out denial-of-service attacks or silently download and install software with the ease of their Twitter-connected smartphones. “All in all, a very slick tool and no doubt script kiddies everywhere are salivating over the prospect of hitting a website with a DDoS from their mobile phones,” a researcher with anti-virus provider Sunbelt Software wrote. TwitterNet Builder requires accounts to be public, so spotting people who use the software is fairly straightforward. A quick search revealed accounts that appeared to be using the DIY kit, although it appeared these might be harmless demonstrations rather than brazen attacks. Regardless, it would be fairly straightforward to modify the tool so it uses private accounts, or even stealthier still, uses base64 encoding so commands appear indecipherable to the naked eye, as a previous Twitter-based bot herders did.
Source: http://www.theregister.co.uk/2010/05/13/diy_twitter_botnets/

50. *May 13, IDG News Service* – (International) **Facebook IDs hacker who tried to sell 1.5M accounts.** Facebook has identified the hacker named Kirillos who tried to sell 1.5

million Facebook accounts recently in underground hacking forums. According to investigators at the social networking site, the hacker is guilty of both hacking and hyperbole. Kirlos was first spotted by researchers at VeriSign's iDefense group a few weeks after he claimed to have an unusually large number of Facebook accounts for sale at rock-bottom prices. According to VeriSign, Kirlos wanted between \$25 and \$45 per 1,000 accounts, depending on the quality of the Facebook user's connections. Kirlos appeared to have sold close to 700,000 accounts, although nobody knew for sure if his claims were legitimate, according to VeriSign's Director of Cyber Intelligence. Now Facebook said its forensics team, working with other industry contacts, has figured out who Kirlos is. A Facebook spokesman would not name Kirlos, but he said that the hacker is based out of Russia. And while Kirlos does appear to have hacked accounts — probably through a phishing attack or by placing malicious code on victims' computers — he probably obtained only a few thousand credentials, the spokesman said.

Source:

http://www.computerworld.com/s/article/9176744/Facebook_IDs_hacker_who_tried_to_sell_1.5M_accounts

51. *May 13, eWeek* – (International) **Facebook makes security changes as privacy controversy swirls.** Amid a controversy about privacy, Facebook unveiled new security features designed to protect user accounts. “Over the last few weeks, we’ve been testing a new feature that allows you to approve the devices you commonly use to log in and then to be notified whenever your account is accessed from a device you haven’t approved,” a software engineer on Facebook’s site integrity team, wrote in Facebook’s blog. To try out the feature, users can go to the Account Settings page and select the option to receive notifications for log-ins from new devices. “When you log in, you’ll be asked to name and save the various devices you use to access Facebook. For example, you can save your home computer, your school or work computer, and your mobile phone. Once you’ve done this, whenever someone logs in to your account from a device not on this list, we’ll ask the person to name the device,” he wrote. Facebook is still dealing with controversy over its privacy policies. A European group of data-protection authorities sent a letter to Facebook May 13, about changes the site made late in 2009 that “fundamentally changed the default settings on its social networking platform to the detriment of a user,” the group charged. Earlier May 13, Facebook had a meeting where employees asked executives questions about privacy. Facebook officials would not comment on exactly what was said in the meeting.

Source: <http://www.eweek.com/c/a/Security/Facebook-Makes-Security-Changes-as-Privacy-Controversy-Swirls-870436/>

52. *May 13, DarkReading* – (International) **E-mail attack targets HR departments.** A targeted attack aimed at human resources departments and hiring managers in the U.S. and Europe that was spotted this week sent 250,000 e-mails during a four-hour period May 12. Researchers at Websense Security Labs discovered the attack, which included the subject line “New resume” and came with a ZIP file attachment and what appeared to be a picture file. When opened, the files spread bot malware and, ultimately, fake antivirus software. “From what the Websense Security Labs has ascertained, the e-mail

campaign would be most relevant to HR departments and managers considering hiring. Employees in these types of roles would most likely be encouraged to view the attachments,” said a senior manager of security research for Websense Security Labs. An executable inside the ZIP file contains the Oficla bot, according to the researchers; the bot connects to a command and control server in the davidopolku.ru domain, and also communicates with topcarmitsubishi.com.br, get-money-now.net, mamapapalol.com, and lili16b0.com. The malware issues a warning message that the victim’s PC is “infected,” and then it downloads the Security Essentials 2010 fake AV program. The researcher said the attackers appear to be trying to make money both by selling fake AV, and by building out a botnet. “This attack installed a downloader onto the infected user’s computer. This means that any payload could be delivered with different directives,” he said.

Source:

<http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=224800010>

53. *May 13, Data Center Knowledge* – (Virginia; National) **Car crash triggers Amazon power outage.** Amazon’s EC2 cloud computing service suffered its fourth power outage in a week May 11, with some customers in its U.S. East Region losing service for about an hour. The incident was triggered when a vehicle crashed into a utility pole near one of the company’s data centers, and a transfer switch failed to properly manage the shift from utility power to the facility’s generators. Amazon Web Services said a “small number of instances” on EC2 lost service at 12:05 p.m. Pacific time May 11, with most of the interrupted apps recovering by 1:08 p.m. The incident affected a different Availability Zone than the ones that experienced three power outages the week of May 3. Amazon Web Services said May 9 that it is making changes in its data centers to address the series of power outages. Amazon EC2 experienced two power outages May 4 and an extended power loss May 8. In each case, a group of users in a single availability zone lost service, while the majority of EC2 users remained unaffected.

Source: <http://www.datacenterknowledge.com/archives/2010/05/13/car-crash-triggers-amazon-power-outage/>

54. *May 12, TechWorld* – (International) **Botnet hijacks web servers for DDoS campaign.** Researchers at Imperva have discovered an “experimental” botnet that uses around 300 hijacked Web servers to launch high-bandwidth DDoS attacks. The servers are all believed to be open to an unspecified security vulnerability that allows the attacker, who goes by the name “Exeman”, to infect them with a tiny, 40-line PHP script. This includes a simple GUI from which the attacker can return at a later date to enter in the IP, port and duration numbers for the attack that is to be launched. But why servers in the first place? Botnets are built from PCs and rarely involve servers. According to Imperva’s CTO, they have no antivirus software and offer high upload bandwidth, typically 10 to 50 times that of a consumer PC. Are there disadvantages to this? There are simply fewer of them, the attacker needs to find vulnerable machines using PHP, and they appear to need manual control, although he did say that attacks could probably be automated using a separate script.

Source: <http://www.networkworld.com/news/2010/051210-botnet-hijacks-web-servers-for.html?hpg1=bn>

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@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

55. *May 13, IDG News Service* – (National) **Lawmaker challenges broadband providers on net neutrality.** If broadband providers do not want the U.S. Federal Communications Commission (FCC) to reclassify broadband as a regulated service, Congress is willing to pass a network neutrality law and address a major reason for reclassification, a senior lawmaker said May 13. Broadband providers have a second option to the FCC Chairman's proposal to reclassify broadband transmission as a common-carrier service, said a democratic U.S. representative from Virginia, who is also chairman of the communications and Internet subcommittee of the House Energy and Commerce Committee. With enforcement of net neutrality rules a major driver for the chairman's reclassification plan, broadband providers instead could work with the subcommittee to craft a net neutrality law, the representative said.

Source:

http://www.computerworld.com/s/article/9176721/Lawmaker_challenges_broadband_providers_on_net_neutrality

56. *May 13, The New New Internet* – (International) **Das internet ist kaputt: German internet disrupted.** Significant portions of the German Internet were unavailable May 12 for over an hour, following a mistake by the DENIC, which administers the .de domain. According to some reports, all 13.6 million .de domains were impacted by the interruption, though other reports said the number of affected domains was smaller. E-mail and Web sites were disrupted from 1:30 p.m. to 2:50 p.m., German time. The problem likely occurred when DENIC uploaded zone files that were empty. "There is no definitive answer," said the CTO of domain registrar name.com. "Best theory right now is an incomplete zone was pushed out." The TLD Source blog said that the problem was a result of the empty zone file uploads. "It looks like they started loading in new zonefiles automatically, having to notice too late that the new zonefile actually didn't contain any information and that they had therefore technically deleted all .de domain names," the blog said.

Source: <http://www.thenewnewinternet.com/2010/05/13/das-internet-ist-kaputt-german-internet-disrupted/>

57. *May 13, San Bernardino Press-Enterprise* – (California) **Pinched cable causes widespread phone, Internet outages from Temecula to Hemet.** A 2.5-hour outage of phone and Internet service across portions of southwest Riverside County May 13 may have started when a fiber-optic cable got pinched in a cabinet door at a substation near Redlands, California according to a Verizon spokesman. The outage affected landlines, cell phone, and Internet service to an unknown number of residents and businesses from Temecula to Hemet. Verizon was still trying to determine the total area affected. The cable got pinched about 2 p.m., and was unable to transmit light through the phone lines. When the door was opened about 4:30 p.m. and the cable became dislodged, service returned to normal to all customers. Phone service was disrupted to police and sheriff's stations in Hemet and Temecula, but the outage did not affect 911 lines. All emergency calls passed through, a sheriff's spokesman said. At the Cal Fire Command Center in Perris, telephone dispatchers were unaffected but Internet service was down. Phones were down at city halls in Temecula, Hemet and San Jacinto, creating busy or disconnected signals for callers. Although the pinched cable was at a facility between San Bernardino and Redlands, police in those two cities reported no outages.

Source:

http://www.pe.com/localnews/stories/PE_News_Local_D_outage14.1a13dab.html

58. *May 12, Television Broadcast* – (New York) **WXXI-TV knocked off the air.** WXXI-TV, the PBS member station serving metro Rochester, New York, was knocked off the air by severe weather. "Due to a transmitter outage caused by recent storm conditions, WXXI DTV 21.1, 21.2 and 21.3 are off the air," WXXI's Web site stated. "Channels are estimated to be back up within the next couple of days. This outage is not affecting cable subscribers." The station's transmitter facility is located in Rochester. The city suffered winds of more than 50 miles per hour over the weekend that took out trees and power lines. Roughly 14,000 of the local utility's customers lost power.

Source: <http://www.televisionbroadcast.com/article/100556>

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

Commercial Facilities Sector

59. *May 14, NBC 4 New York* – (New York) **All clear after Union Square bomb scare.** New York City police (NYPD) evacuated part of an apartment building and blocked off some streets near Manhattan's Union Square after a May 13 report of a suspicious vehicle with gas in the back seat, but nothing threatening was found. NYPD investigators located the owner of the 1991 Oldsmobile Cutlass Ciera, which was parked in front of the Con Edison utility building around 10 p.m. He told police he had the gas cans in his car because he mows lawns for his family. He parked the car in the area because he was attending a concert nearby, police said. The bomb squad suited up and began an investigation after a Con Edison employee called 911 to report the vehicle as suspicious because of the two gas cans in the back seat on the floor. Several floors of a high-rise residential building were evacuated and some streets in the area were blocked off as a precaution.

Source: <http://www.nbcnewyork.com/news/local-beat/Scare-Shuts-Down-Streets-Near-Union-Square-93743624.html>

60. *May 13, Associated Press* – (California) **Part of Disneyland cleared due to unclaimed bag.** A part of Disneyland in Anaheim was briefly evacuated because of a suspicious bag spotted near a ride. An Anaheim police sergeant said May 12 about 1,000 people were asked to leave Tomorrowland for about 90 minutes because of the unclaimed bag. A bomb squad determined the bag — described as a rolling ice chest — was harmless and contained food. The bag was near the Captain EO ride in an area not accessible to the public. Disney employees are being let back in, and no other areas of the park were affected.
Source: <http://www.google.com/hostednews/ap/article/ALeqM5gSDCtYc3Cjv02jzERBgwPi9TMqQwD9FLKTB80>
61. *May 12, Bristol Herald Courier* – (Virginia) **Two Walmart employees arrested, accused of calling in bomb threats.** Two Walmart employees were arrested at work late May 11, accused of calling in at least a dozen bomb threats to the Bristol, Virginia superstore over the past week, and as many as eight in one day. The Washington County sheriff said the pair used one cell phone to make the calls. He declined, however, to release investigation details. After the first threat, called into the pharmacy around lunchtime May 5, management evacuated the store for several hours as bomb-sniffing dogs and employees hunted for the nonexistent explosives. The evacuation cost the store between \$40,000 and \$50,000 in lost profits. The next call came into Walmart's Tire and Lube Express May 8. The store remained open, but the car service center closed until the following day. That closure cost the chain about \$10,000. There were eight more threats May 10, and two May 11. The two suspects work the evening shift at the Tire and Lube Express and, about 10 p.m. May 11, were arrested on the job. Each are charged with one count of making and communicating a threat to bomb, burn, destroy or damage a building. Additional charges are pending. No evidence of bombs or bomb-making supplies have been found at the Walmart.
Source: http://www2.tricity.com/tri/news/local/article/two_walmart_employees_arrested_accused_of_calling_in_bomb_threats/46099/

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

National Monuments and Icons Sector

62. *May 14, Associated Press* – (South Dakota) **Black Hills National Forest roads to stay closed.** Wet weather is causing road problems in the Black Hills National Forest. Seasonally closed roads were to be reopened for summer use May 14, but the U.S. Forest Service said many roads will remain closed to traffic this weekend. Both rain and recent snowfall have made for difficult, muddy conditions on dirt roads and made them susceptible to damage. Roads will be reopened as soon as they dry out.
Source: <http://cbs4denver.com/wireapnews/Many.Black.Hills.2.1694036.html>

Dams Sector

63. *May 13, Fly Rod and Reel* – (National) **American Rivers releases plan for better flood management.** American Rivers voiced support May 13 for efforts to help communities across Tennessee, Kentucky, and Mississippi recover from recent floods, and released a four point plan to prevent dangerous and damaging floods in the future. American Rivers highlighted four priorities that are an essential part of a 21st century flood-management plan. 1) Remove or repair unsafe dams. As in all parts of the United States, there are many unsafe or obsolete dams throughout the Southeast. These dams can make flooding worse by increasing flood heights upstream or, in the worst case scenario, when the dam fails. 2) Restore and protect floodplains. Protecting and restoring natural floodplains gives rivers room to spread out, which reduces flood levels. Allowing rivers to overflow onto natural floodplains upstream of populated areas can also help alleviate pressure on levees guarding cities. High-risk facilities like hospitals, schools and elder housing should never be developed in floodplains. 3) Protect wetlands. Wetlands are nature's sponges, absorbing floodwaters and releasing them slowly over time. Even having four to five percent wetland coverage in a watershed can reduce peak floods by 50 percent. Wetlands that are drained, filled, or isolated behind levees provide little or no flood protection for the surrounding community. 4) Reform flood insurance. Congress originally intended the National Flood Insurance Program to reduce the nation's vulnerability to flood damage. Instead, the program has run up a near \$20 billion debt to the federal treasury and has encouraged destruction of floodplains and wildlife habitat, with taxpayer subsidies. Congress must use the upcoming National Flood Insurance Program law reauthorization to reform the program in order to ensure fiscal solvency, public safety, and river health.

Source: <http://www.flyrodreel.com/blogs/tedwilliams/2010/may/american-releases-management>

64. *May 13, Peoria Journal Star* – (Illinois) **Heavy rain swells Spoon River.** Heavy rains in Fulton County, Illinois, caused one levee to break May 13, and London Mills residents are being cautioned about the rising Spoon River. The levee breach north of Illinois Route 9 was repaired later in the day, according to the Fulton County Emergency Service Disaster Agency director, but the Spoon River was steadily rising. A flood warning for the Spoon River was issued Thursday by the National Weather Service (NWS). According to NWS, flood stage for the Spoon River at London Mills is 15 feet. At 7:45 p.m., the river was at 18.59 feet and was expected to crest at 22.9 feet at about 8 p.m. Friday. Three rural roads had been closed for a distance of a mile or so and will remain closed until at least Friday morning.

Source: <http://www.pjstar.com/news/x1773731877/Heavy-rain-swells-Spoon-River>

65. *May 12, Hydro World* – (International) **Two killed in blast at Russian hydropower plant.** An explosion May 12 at a hydropower plant in central Russia killed two people, including a firefighter, and injured 10 workers, wire services reported. A regional

emergency official said the blast occurred at the Lower Kama hydropower plant in the Tatarstan region, some 1,000 kilometers (600 miles) east of Moscow. A compressor exploded in the turbine room, but the cause of the accident was not immediately clear, investigating agencies said in a statement. Smoke appeared in the turbine room about 10 minutes before the explosion, state news agencies reported, citing the Energy Ministry. The turbine shop director was killed, as was a firefighter who fell from a height during the rescue operation, investigators said. The incident did not affect the normal operation of the plant, local media reported.

Source: http://www.hydroworld.com/index/display/article-display/5068281173/articles/hrhrw/News-2/2010/05/two-killed_in_blast.html

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

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 ten days on the Department of Homeland Security Web site: <http://www.dhs.gov/iaipdailyreport>

Contact Information

Content and Suggestions:

Send mail to NICCRports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421

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@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.