



Homeland
Security

Daily Open Source Infrastructure Report

12 November 2014

Top Stories

- The U.S. Postal Service announced November 10 that the personal information of more than 800,000 employees and customers were potentially accessed in a cyberattack. – *Reuters* (See item [8](#))
- Thousands of food products worth more than \$3 million were scattered all over the roadway following an accident on Interstate 24 east near Monteagle, Tennessee, shutting down the interstate for more than 4 hours November 9. – *Chattanooga Times Free Press* (See item [9](#))
- Researchers identified an advanced persistent threat (APT) group dubbed Darkhotel APT that has targeted travelers in the Asia-Pacific region using malicious hotel WiFi networks, spear phishing, and malicious torrent files. – *Securityweek* (See item [26](#))
- About 5,000 people were evacuated from office buildings or told to shelter-in-place in San Jose, California, November 7 – November 8 while crews worked to repair a 4 inch natural gas pipeline that was inadvertently struck. – *San Jose Mercury News* (See item [35](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

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

SUSTENANCE and HEALTH

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

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
-

Energy Sector

See item [26](#)

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

Chemical Industry Sector

Nothing to report

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

Nuclear Reactors, Materials, and Waste Sector

1. *November 7, Cleveland Plain Dealer* – (Ohio) **Perry nuclear power plant shut itself down Friday morning without incident.** The reactor at the Perry nuclear power plant in North Perry experienced an automatic shutdown November 7. A preliminary investigation determined that a voltage issue in one of the electrical panels that supplies power to cooling pumps was the cause of the shutdown.

Source:

http://www.cleveland.com/business/index.ssf/2014/11/perry_nuclear_power_plant_shut_1.html

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

Critical Manufacturing Sector

2. *November 8, Associated Press* – (National) **Nissan recalls 52,000 vehicles for faulty air bags.** Nissan announced November 8 that it is recalling 52,738 Nissan and Infiniti vehicles due to airbag inflators manufactured by Takata Corp., which could explode upon airbag deployment and send metal shards into the passenger compartment. Affected models include model year 2003-2004 Nissan Pathfinder, 2004-2006 Sentra, 2003-2005 Infiniti FX 35 and FX 45, 2003-2004 I35, and 2006 M35 and M45 vehicles.

Source: <http://woodtv.com/2014/11/08/nissan-recalls-52000-vehicles-for-faulty-air-bags/>

3. *November 7, Associated Press* – (California) **Convicted felon arrested in scheme to embezzle \$8.5 million as Gulfstream finance director.** The former finance director of Gulfstream Aerospace Corp.'s Long Beach and Las Vegas operations was arrested November 7 and charged with allegedly using fake companies to bill Gulfstream for at least \$8.5 million in fraudulent charges and using the stolen funds for his personal use. The Calabasas man was fired by Gulfstream in 2013 after the company found that he had lied on a 2000 application regarding a conviction for embezzling \$2.4 million from a previous employer.

Source: <http://www.foxnews.com/us/2014/11/07/convicted-felon-arrested-in-scheme-to-embezzle-85-million-as-gulfstream-finance/>

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

Defense Industrial Base Sector

See item [26](#)

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

Financial Services Sector

4. *November 7, WSB 750 AM Atlanta* – (Georgia) **Massive credit card scam found in Paulding Co.** Authorities in Paulding County arrested a Kennesaw man for allegedly operating a payment card forgery operation after police were contacted by the owner of an office building who had discovered suspicious items while cleaning out the office space of an evicted tenant. Police found 1,154 payment cards as well as card embossing devices and several fraudulent driver's licenses from various States.
Source: <http://www.wsbradio.com/news/news/local/massive-credit-card-scam-found-paulding-co/nh3C3/>
5. *November 7, Amarillo Globe-News* – (Texas) **Troopers seize nearly \$200k in fake credit cards, cash.** Texas Department of Public Safety troopers arrested two Romanian nationals after they found 69 fraudulent payment cards valued at \$172,000 and 29 fraudulent ID cards from Iowa during a traffic stop in Carson County November 4. Troopers stated that they believed the contraband and \$18,000 in cash was being transported from California to Tennessee.
Source: <http://amarillo.com/news/local-news/2014-11-07/troopers-seize-nearly-200k-fake-credit-cards-cash>
6. *November 7, KIRO 7 Seattle* – (Washington) **'Roscoe Bandit' strikes Olympia bank.** A suspect known as the "Roscoe Bandit" linked to two bank robberies in Seattle was also linked to an October 30 robbery of Timberland Bank in Olympia. The previous Seattle robberies occurred July 29 at a Wells Fargo Bank branch and July 28 at a HomeStreet Bank branch.
Source: <http://www.kirotv.com/news/news/roscoe-bandit-strikes-olympia-bank/nh3SQ/>
7. *November 7, Chicago Sun-Times* – (Illinois) **'Bully Bandit' suspected of three more bank robberies.** The FBI is offering a reward for information on the "Bully Bandit" after the suspect was linked to 3 additional robberies in the Chicago area, bringing the suspect's total to 15 bank robberies since 2012. The most recent bank robbery occurred November 5 at a Chase Bank branch in Chicago.
Source: <http://www.myfoxchicago.com/story/27326638/bully-bandit-suspected-of-three-more-bank-robberies>

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

Transportation Systems Sector

8. *November 10, Reuters* – (National) **U.S. Postal Service says data breach hits employees, call center.** The U.S. Postal Service (USPS) announced November 10 that the personal information, including Social Security numbers, of more than 800,000 employees and customers who called the Postal Service Customer Care Center between January and August 16 was potentially accessed in a cyberattack. The USPS is investigating and reported that the intrusion is limited in scope and operations are functioning normally.
Source: <http://www.reuters.com/article/2014/11/10/us-cybersecurity-usps-idUSKCN0IU1P420141110>
9. *November 10, Chattanooga Times Free Press* – (Tennessee) **Meat, eggs and cheese only casualties of I-24 pileup on Monteagle.** Thousands of eggs, cheese, and boxes of meat worth more than \$3 million collectively were scattered all over the roadway following an accident between 3 semi-trucks and 2 cars on Interstate 24 east near Monteagle, shutting down the interstate for more than 4 hours November 9 while crews cleared the scene. One driver was injured in the incident.
Source: <http://www.timesfreepress.com/news/2014/nov/10/meat-eggs-and-cheese-only-casualties-of-i-24/>
10. *November 10, WFMZ 69 Allentown* – (Pennsylvania) **Route 61 in Hamburg closed for hours after U.S. mail truck accident.** Southbound lanes of Route 61 in Berks County were closed for nearly 8 hours after a U.S. mail truck swerved off the roadway and plummeted down an 80 foot embankment in an effort to miss hitting a deer. Officials reported that some of the mail products were damaged.
Source: <http://www.wfmz.com/news/news-regional-berks/route-61-in-hamburg-closed-after-us-mail-truck-accident/29627686>
11. *November 8, Charlotte Observer* – (North Carolina) **Train slams into lettuce truck in Bessemer City.** A portion of the Norfolk Southern tracks in Bessemer City were closed for approximately 3 hours for cleanup November 8 following a collision between a semi-truck carrying lettuce and a train at a rail road crossing on South 8th Street.
Source: <http://www.charlotteobserver.com/2014/11/08/5301761/train-slams-into-lettuce-truck.html>
12. *November 6, WITI 6 Milwaukee* – (Wisconsin) **Semi rollover leads to extreme backups on I-94/43 in Plainfield Curve.** A semi-truck carrying 78,000 pounds of grain overturned and crashed into a light pole leading to the closure of 2 northbound and 2 southbound lanes of Interstate 43 near Howard Avenue in Milwaukee for 6 hours November 6.
Source: <http://fox6now.com/2014/11/06/traffic-alert-wreck-slows-traffic-to-a-crawl-in-plainfield-curve/>

Food and Agriculture Sector

13. *November 9, U.S. Department of Agriculture* – (Hawaii) **Hawaii firm recalls frozen pork products due to misbranding and undeclared allergen.** The Food Safety and Inspection Service reported November 9 that Kulana Foods Ltd., issued a recall for about 4,465 pounds of Mountain Apple Brand Teri Smoked Pork products due to undeclared wheat caused by misbranding. The products were distributed to retailers and foodservice locations on the islands of Hawaii and Oahu.
Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2014/recall-077-2014-release>
14. *November 8, U.S. Food and Drug Administration* – (International) **Marin Food Specialties, Inc. initiates voluntary recall of imported Organic Raw Almonds (bitter almonds) due to elevated levels of naturally occurring hydrogen cyanide.** The U.S. Food and Drug Administration announced November 7 that Marin Foods Specialties, Inc., issued a recall of its Organic Raw Almonds (bitter almonds) due to the possibility that they contain elevated levels of naturally occurring hydrogen cyanide based on laboratory test results. The products were imported from Italy and Spain and sold in 13.5 ounce containers at Whole Foods Market stores in California, Oregon, Washington, Nevada, and Idaho.
Source: <http://www.fda.gov/Safety/Recalls/ucm422431.htm>
15. *November 8, Food Safety News* – (National) **Recalled bean sprouts linked to 2 Listeria deaths, 3 hospitalizations.** The U.S. Centers for Disease Control and Prevention reported that 2 individuals died and 3 others were hospitalized between June and August after consuming Wholesome Soy Products-branded bean sprouts that were determined to be contaminated with *Listeria monocytogenes*. The Illinois Department of Public Health is working to embargo all products from the company after follow-up inspections by the U.S. Food and Drug Administration revealed additional environmental samples with *Listeria* contamination.
Source: <http://www.foodsafetynews.com/2014/11/recalled-bean-sprouts-linked-to-2-listeria-deaths-3-hospitalizations>

For another story, see item [9](#)

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

Water and Wastewater Systems Sector

16. *November 9, Orange County Register* – (California) **Sewage spill closes 15 docks in Dana Point.** Orange County Health Care Agency officials announced a no swimming and diving advisory until further notice November 9 following a sewage spill that led to the closure of 15 docks in Dana Point Harbor after tests came back positive for elevated levels of bacteria. The advisory also warned beachgoers to avoid contact with the water at Harbor Tower Marina, Pacific Coast Highway, and Newport Boulevard due to potential urban runoff.
Source: <http://www.ocregister.com/articles/dana-641455-harbor-point.html>

17. *November 9, KIRO 7 Seattle* – (Washington) **Sewage spill in Silverdale, no-contact advisory through Monday.** A no-contact advisory was issued for the Silverdale waterfront covering the recreation area and fresh and storm water drainage areas to the shoreline in Washington November 7 through November 10 following a sewage leak in Old Town Silverdale.
Source: <http://www.kirotv.com/news/news/sewage-spill-silverdale-no-contact-advisory-throug/nh3xC/>
18. *November 8, Associated Press* – (Texas) **Broken pipeline spills wastewater in Austin.** Approximately 100,000 gallons of wastewater spilled in Austin after a contractor struck an underground pipeline November 7. Crews were able to contain the spill from entering any creeks or tributaries in the area and the line was expected to be repaired by November 8.
Source: <http://www.ksat.com/content/pns/ksat/news/2014/11/08/broken-pipeline-spills-wastewater-in-austin.html>

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

Healthcare and Public Health Sector

19. *November 10, WMUR 9 Manchester* – (New Hampshire) **Bristol police search for armed robber who stole pills from pharmacy.** Bristol police are searching for a suspect who robbed a Rite Aid pharmacy on Summer Street at gunpoint November 9 and stole about 1,100 OxyContin pills.
Source: <http://www.wmur.com/news/bristol-police-search-for-armed-robber-who-stole-pills-from-pharmacy/29634920>
20. *November 7, Securityweek* – (North Carolina) **N.C. dermatology center discovers hacked server two years after attack.** Central Dermatology Center in Chapel Hill announced November 7 that one of its servers was breached and compromised by malware in August 2012. The health center discovered the breach September 25 and continues to investigate the attack in order to determine what information was compromised, which could include patients' personal and medical information.
Source: <http://www.securityweek.com/nc-dermatology-center-discovers-hacked-server-two-years-after-attack>

For additional stories, see items [25](#) and [26](#)

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

Government Facilities Sector

21. *November 10, Pittsburgh Tribune-Review* – (Pennsylvania) **Franklin Regional High School students sent home after bomb threat.** Students were evacuated and classes were dismissed at Franklin Regional High School in Murrys ville due to a bomb threat November 10. Authorities reported to the campus to investigate.

Source: <http://triblive.com/news/adminpage/7126828-74/threat-students-sent>

22. *November 8, Associated Press* – (Wyoming) **Hackers breach Wyoming library system.** Officials announced November 7 that the Statewide online catalog of the Wyoming State Library was taken offline for 2 days for remediation after authorities learned the system was breached October 7 by unknown hackers. The attack was discovered after unusual activity was detected on the system and there is no indication that personal data was compromised.

Source: <http://www.kansas.com/news/business/article3661611.html>

23. *November 7, Orange County Register* – (California) **Power restored at CSUF; classes canceled, but university functions unaffected.** Classes at California State University, Fullerton were cancelled November 7 following a power outage on campus. Crews restored service after several hours and all university functions resumed normal operations.

Source: <http://www.ocregister.com/articles/outage-641250-reported-power.html>

For another story, see item [26](#)

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

Emergency Services Sector

24. *November 9, WKYC 3 Cleveland* – (Ohio) **Six Cleveland officers suspended after investigation.** The Cleveland Police Patrolman's Association confirmed that six Cleveland Police Department officers were suspended after a months-long investigation uncovered that the officers were leaving work zones during assigned patrol and filing false duty reports.

Source: <http://www.wkyc.com/story/news/local/cleveland/2014/11/08/6-officers-suspended-after-gas-station-investigation/18743773/>

25. *November 7, WMTW 8 Poland Spring* – (Maine) **Jail workers supposed to get TB test, get flu shot instead.** Cumberland County Jail in Portland, Maine, reported November 7 that 41 correctional officers inadvertently received flu vaccinations instead of a tuberculosis test November 4. Corizon Health, a sub-contracting medical firm, launched an investigation after two nurses did not follow proper medical procedures and administered the wrong shots.

Source: <http://www.wmtw.com/news/jail-workers-supposed-to-get-tb-test-get-flu-shot-instead/29580468>

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

Information Technology Sector

26. *November 10, Securityweek* – (International) **Darkhotel attackers target business travelers via hotel networks.** Kaspersky Lab researchers identified an advanced persistent threat (APT) group dubbed Darkhotel APT that has targeted travelers in the

Asia-Pacific region in addition to the U.S. using malicious hotel WiFi networks, spear phishing, and malicious torrent files. The group's hotel attacks involve prompting users with a software update notice that installs a backdoor, and the group has targeted guests associated with industries and sectors including government organizations, the defense industry, energy industry, pharmaceutical industry, electronics manufacturers, medical providers, and non-governmental organizations.

Source: <http://www.securityweek.com/darkhotel-attackers-target-business-travelers-hotel-networks>

27. *November 10, The Register* – (International) **BrowserStack HACK ATTACK: Service still suspended after rogue email.** Browser testing service BrowserStack stated that it was temporarily suspending service to recover after an attacker managed to gain access to a list of email addresses and the company's official email account, using it to send out a fake message to developers.
Source: http://www.theregister.co.uk/2014/11/10/browserstack_hack_attack_service_still_suspended_after_rogue_email/
28. *November 10, The Register* – (International) **Emoticons blast three security holes in Pidgin :-).** Researchers at Cisco reported that the instant messaging client Pidgin contained three security vulnerabilities that could have allowed attackers to overwrite files or cause a denial of service (DoS) situation. The vulnerabilities have since been patched.
Source: http://www.theregister.co.uk/2014/11/10/cisco_security_bods_hunt_pidgin/

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: <http://www.it-isac.org>

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

Communications Sector

29. *November 10, Lancaster Online* – (Pennsylvania) **579 people in Lancaster County lose phone service after vehicle crash.** Approximately 579 Frontier Communications customers from Quarryville to Caernarvon Township in Lancaster County were without phone service for several hours November 9 after a vehicle struck and damaged a pole at the intersection of Routes 340 and 772.
Source: http://lancasteronline.com/news/local/people-in-lancaster-county-lose-phone-service-after-vehicle-crash/article_d50be6ba-6834-11e4-8ea5-338b6a11f59f.html
30. *November 8, Honolulu Star-Advertiser* – (Hawaii) **140 Hawaiian Telecom customers now without service in Kaimuki.** A phone and high-speed Internet service disruption October 21 continued for 140 Hawaiian Telecom customers in the Kaimuki and

Maunalani Heights areas of east Honolulu November 8 following a break in a 12 inch water main that pushed several feet of asphalt, debris, and rocks into an open manhole covering underground cables. Crews continued work to remove the debris in order to restore service.

Source:

http://www.staradvertiser.com/news/breaking/20141108_140_Hawaiian_Telcom_customers_now_without_service_in_Kaimuki.html?id=282056391

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

Commercial Facilities Sector

31. *November 10, WWLP 22 Springfield* – (Massachusetts) **20 still can't go home after Agawam apartment complex fire.** Twenty residents of the Shibley Court Apartments in Agawam were displaced following a November 9 fire that destroyed one apartment unit and damaged several others. About 70 residents were temporarily evacuated from at least 3 of the complex's structures while firefighters battled the blaze.
Source: <http://wwlp.com/2014/11/10/apartment-fire-leaves-an-estimated-20-people-with-a-home/>
32. *November 9, WBBM 2 Chicago* – (Illinois) **10-year-old boy killed, 11 hurt in fire on northwest side.** One resident died and 11 others were injured in a 3-alarm fire that broke out November 9 at an apartment building in the Hollywood Park neighborhood of Chicago. The cause of the fire is under investigation.
Source: <http://chicago.cbslocal.com/2014/11/09/10-year-old-boy-killed-11-hurt-in-northwest-side-fire/>
33. *November 8, San Jose Mercury News* – (California) **Redwood City: Norovirus to blame for Hotel Sofitel sickness outbreak.** San Mateo County health officials reported November 7 that norovirus was the source of an outbreak that sickened at least 60 hotel guests and employees at 3 special events taking place at the Hotel Sofitel in Redwood Shores beginning October 26. The hotel stopped serving food and sanitized the property before partially resuming food service November 3.
Source: http://www.mercurynews.com/san-mateo-county-times/ci_26894492/redwood-city-norovirus-blame-hotel-sofitel-sickness-outbreak
34. *November 8, WCPO 9 Cincinnati* – (Ohio) **Middletown apartment fire displaces 32 people.** A November 8 fire at an apartment complex in Middletown, Ohio, displaced 32 residents and caused an estimated \$300,000 in damage to the structure which was rendered a total loss. Authorities are investigating the cause of the fire.
Source: <http://www.wcpo.com/news/local-news/butler-county/middletown/middletown-apartment-fire-displaces-32-people>
35. *November 8, San Jose Mercury News* – (California) **San Jose: All-clear given after downtown natural-gas leak.** About 2,500 people were evacuated from office buildings in downtown San Jose and around 2,500 additional people were ordered to

shelter-in-place November 7 while crews worked to repair a 4 inch natural gas pipeline that was inadvertently struck by a construction crew working in the area. The scene was cleared November 8 after HAZMAT crews tested buildings for possible pockets of gas that could be trapped inside, and service was expected to be restored to the 40 affected businesses by November 10.

Source: http://www.mercurynews.com/bay-area-news/ci_26898555/san-jose-bus-lines-resume-normal-service-after

36. *November 7, Associated Press* – (Texas) **Explosion rocks Texas border town.** Crews worked November 7 to restore power to about 145 mainly commercial customers in Laredo that lost service following a fire in an underground electrical network November 6 that caused flames to erupt from at least 2 manholes.

Source: <http://www.mysanantonio.com/news/local/article/Explosion-rocks-Texas-border-town-5878178.php>

For another story, see item [26](#)

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

Dams Sector

Nothing to report

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



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) 942-8590
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.