



Daily Open Source Infrastructure Report 11 May 2016

Top Stories

- A loan officer and three others were indicted on Federal charges May 9 after the group allegedly defrauded several central Kentucky banks out of more than \$40 million in loans or loan renewals. – *Lexington Herald-Leader* (See item [5](#))
- Researchers at Proofpoint discovered CryptXXX version 2.006 which defeats a Kaspersky Lab decrypter, and locks a user’s entire screen, forcing them to log onto a different computer to go online to buy Bitcoin and pay the ransom. – *Softpedia* (See item [20](#))
- The U.S. Federal Trade Commission began an investigation May 10 into the security practices of eight major mobile companies to determine how the companies plan and carry out security operations for their mobile divisions. – *Softpedia* (See item [21](#))
- Los Angeles Police are searching for 5 men suspected of stealing over 7,600 Dell laptop computers worth approximately \$4 million May 6 from a warehouse in the Harbor Gateway area. – *MyNewsLA.com* (See item [23](#))

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

1. *May 9, Forum of Fargo-Moorhead* – (North Dakota) **Officials target source of saltwater spill near Parshall.** North Dakota authorities announced May 9 that 10,878 gallons of saltwater was released May 7 from an EOG Resources, Inc., central tank battery site in Mountrail County when the fitting on a hose failed. EOG Resources reported that the spill was contained on location and all but 420 gallons have been recovered.
Source: <http://www.inforum.com/news/4028305-officials-target-source-saltwater-spill-near-parshall>
2. *May 9, Alaska Dispatch News* – (Alaska) **Worker with wrench sparked fire that shut down Alaska oil pipeline, company says.** An official with Alyeska Pipeline Service Co., released preliminary findings May 9 on an April 20 fire at the trans-Alaska oil pipeline near Coldfoot stating that the fire occurred when an adjustment wrench, being used by a pipeline technician to loosen some nuts on a metal access plate, slipped and struck a metal object. The incident at Pump Station 5 released flames into the air and shut down the pipeline for nine hours.
Source: <http://www.adn.com/article/20160509/worker-wrench-sparked-fire-shut-down-alaska-oil-pipeline-company-says>

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

3. *May 9, TheCarConnection.com* – (International) **2009-2016 Dodge Journey recalled for steering problems.** Fiat Chrysler Automobiles issue a recall May 9 for 10,944 of its model years 2009 – 2016 Dodge Journey vehicles equipped with optional block heaters sold in the U.S. due to a steering issue where lines carrying power-steering fluid may leak when starting the engine in cold temperatures, thereby making the vehicle more difficult to steer and increasing the risk of a crash. No injuries have been reported in connection with the recall which includes an additional 187,436 vehicles sold in Canada.
Source: http://www.thecarconnection.com/news/1103852_2009-2016-dodge-journey-recalled-for-steering-problems
4. *May 9, U.S. Department of Labor* – (Georgia) **Plastics manufacturer exposes employees to amputation, other hazards; OSHA proposes \$54K in fines after Federal safety and health inspection.** The Occupational Safety and Health Administration cited Thomson Plastics Inc., with one repeat and two serious safety violations May 9 after an inspection at the Thomson, Georgia facility revealed that the

company failed to perform annual inspections of its energy control procedures, and failed to provide written energy control procedures to prevent machinery start-ups during service and maintenance, among other violations. Proposed penalties total \$54,000.

Source:

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=31791

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *May 9, Lexington Herald-Leader* – (Kentucky) **Four charged in alleged central Kentucky bank fraud involving \$40 million.** A loan officer and three others were indicted on Federal charges May 9 after the group, operating as various businesses, allegedly defrauded several central Kentucky banks out of more than \$40 million in loans or loan renewals by making false representations or omissions on loan documents to banks in Fayette, Woodford, and Harrison counties from May 2006 – September 2010. Officials stated that the group used the loans for purposes other than those listed in the application.

Source: <http://www.kentucky.com/news/local/crime/article76606412.html>

6. *May 9, SecurityWeek* – (International) **Android trojan steals credit card info, locks devices remotely.** Researchers from Avast discovered a new Android banking trojan that is capable of spying on users and stealing credit card information by gaining admin rights to a victim's device after continuously prompting the Device Admin activation dialog until the user grants the malware admin rights, while hiding the app icon following the program's first run. Researchers stated that the trojan is designed to send information about the device to a command and control (C&C) server, intercept incoming short message service (SMS) messages and send them to the server, and receive further commands from its operators.

Source: <http://www.securityweek.com/android-trojan-steals-credit-card-info-locks-devices-remotely>

Transportation Systems Sector

7. *May 9, CNN* – (Tennessee) **Missing engine cover prompts Delta flight's emergency landing.** A Delta Air Lines flight traveling from Atlanta to Chicago was forced to make an emergency landing in Nashville May 8 after the cowling, a piece covering the plane's right engine, separated from the plane and struck part of the fuselage. No injuries were reported.

Source: <http://www.cnn.com/2016/05/09/aviation/delta-flight-emergency-landing-engine-cover-trnd/>

8. *May 9, WTAJ 10 Altoona* – (Pennsylvania) **Three killed in highway crash.** A portion

of Interstate 80 westbound in Union Township, Pennsylvania, was closed for several hours May 9 while authorities investigated a multi-vehicle crash that left three people dead.

Source: <http://www.wearecentralpa.com/news/three-killed-in-highway-crash>

9. *May 9, WTVF 5 Nashville* – (Tennessee) **Victim ID'd in 5-vehicle crash on Highway 109.** Highway 109 north in Wilson County, Tennessee, was closed for several hours May 8 after a vehicle traveling northbound rear-ended a vehicle in front of it, causing a chain reaction crash that involved five vehicles, left one person dead, and sent two others to an area hospital with injuries.

Source: <http://www.newschannel5.com/traffic/crash-in-wilson-county-shuts-down-highway-109>

For another story, see item [2](#)

Food and Agriculture Sector

10. *May 9, U.S. Department of Labor* – (Massachusetts) **Ammonia leak, alarm failure at Taunton food products distribution center highlights potentially deadly chemical hazard.** The Occupational Safety and Health Administration cited Reinhart Food Service, LLC with six serious and two repeated health violations April 20 after an employee complaint prompted an inspection at the Taunton, Massachusetts facility which revealed that a check valve in the facility's pump room leaked nine pounds of anhydrous ammonia in addition to several other deficiencies in the company's Process Safety Management program including an inadequate emergency response plan, and inadequate procedures for inspecting, testing, and replacing valves and ammonia sensors. Proposed penalties total \$72,000.

Source:

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=31785

11. *May 9, U.S. Food and Drug Administration* – (National) **Let's Talk Health, Inc. issues allergy alert on undeclared milk and soy in Energizer Drink Mix.** Let's Talk Health, Inc., issued a recall May 9 for 15 packet jars of its Energizer Drink Mix products sold in 3 variations, and its Agua Vitae Liquid Multi-Vitamin, Aqua Vitae Kids Liquid Multi-Vitamin, and Tox-Elim Liquid products due to undeclared milk and soy allergens after it was discovered that a whey protein ingredient was used in the products following a temporary breakdown in the manufacturing company's production and packaging processes. No illnesses have been reported and the products were distributed to retail stores and through mail orders nationwide.

Source: <http://www.fda.gov/Safety/Recalls/ucm499977.htm>

12. *May 9, U.S. Food and Drug Administration* – (National) **Kroger recalls broccoli raisin salad after supplier Listeria concern.** The Kroger Co., issued a recall May 9 for its Kroger Broccoli Raisin Salad products due to a potential *Listeria monocytogenes* contamination after the company was notified by its sunflower kernels supplier that the kernels may be contaminated with *Listeria*. The products were removed from store

shelves and no illnesses have been reported in connection with the products which were sold at 6 different store chains in 19 States.

Source: <http://www.fda.gov/Safety/Recalls/ucm499961.htm>

13. *May 9, U.S. Food and Drug Administration* – (National) **Bickel’s Snack Foods recalls Golden Gourmet Veggie Chips because of possible health risk.** Bickel’s Snack Foods Inc., issued a voluntary recall May 5 for 2,010 bags of its Golden Gourmet Veggie Chips products due to mislabeling and undeclared milk after it was discovered during stocking at the retail level that a Golden Gourmet Veggie Chips package contained Golden Gourmet Ranch Flavored Veggie Chips products, which are made with milk. No illnesses have been reported and the products were distributed to retail locations in 29 States.
Source: <http://www.fda.gov/Safety/Recalls/ucm499931.htm>

14. *May 9, U.S. Food and Drug Administration* – (National) **Food recall of sweet and salty trail mix – because of possible health risk, due to potential presence of Listeria monocytogenes.** Rucker’s Wholesale and Service Co., issued a voluntary recall May 9 for its Uncle Bucks Sweet & Salty Trail Mix peg bag products sold in 3-ounce packages due to a potential Listeria monocytogenes contamination after the company was notified by its sunflower kernel supplier that the kernels used in the trail mix products may be contaminated with Listeria. No illnesses have been reported and the products were distributed to Bass Pro Shops stores nationwide.
Source: <http://www.fda.gov/Safety/Recalls/ucm500009.htm>

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

15. *May 10, Syracuse Post-Standard* – (New York) **Legionnaires’ case prompts Auburn nursing home to restrict water use.** The Commons at St. Anthony nursing home in Auburn placed filters on shower faucets, restricted water use, and is undergoing additional remediation efforts May 10 after Legionella bacteria was found in the nursing home’s drinking water system when a resident tested positive for Legionnaires’ disease.
Source:
http://www.syracuse.com/health/index.ssf/2016/05/legionnaires_case_prompts_auburn_nursing_home_to_restrict_water_use.html

Government Facilities Sector

16. *May 9, Detroit Free Press* – (Michigan) **Central High in Detroit closed because of water pressure issues.** Low water pressure prompted the closure of Central High School in Detroit May 4 – May 10. Officials stated that crews were working to install a temporary water line to the school.
Source: <http://www.freep.com/story/news/education/2016/05/09/central-water->

[problem/84160210/](#)

17. *May 9, Washington Post* – (Massachusetts) **Tufts University resumes limited operations after morning bomb threat.** Tufts University in Massachusetts resumed limited operations May 9 after several buildings were evacuated, searched, and deemed safe following a car fire and bomb threat that prompted the university to postpone final exams and ask students and faculty to remain indoors.
Source: <https://www.washingtonpost.com/news/grade-point/wp/2016/05/09/bomb-threat-car-fire-at-tufts-university-under-investigation/>

Emergency Services Sector

18. *May 10, Associated Press* – (New Jersey) **Inmate captured just shy of parole, faces more prison time.** Authorities recaptured an inmate May 9 near the Garden State Parkway in New Jersey after he escaped from the Ancora unit of Bayside State Prison in Hammonton May 3.
Source: <http://abcnews.go.com/US/wireStory/inmate-captured-shy-parole-faces-prison-time-39000835>

Information Technology Sector

19. *May 10, Softpedia* – (International) **SS7 attack leaves WhatsApp and Telegram encryption useless.** Positive Technologies researchers unveiled a new attack that utilizes Signaling System No. 7 (SS7) to carry out attacks on encrypted communications apps such as WhatsApp and Telegram by spoofing a mobile network node and intercepting the initial phase of a chat between two users. The researchers were able to impersonate a second user through SS7 loopholes that were never patched.
Source: <http://news.softpedia.com/news/ss7-attack-leaves-whatsapp-and-telegram-encryption-useless-503894.shtml>
20. *May 10, Softpedia* – (International) **CryptXXX is now undecryptable, prevents users from accessing their PC.** Researchers at Proofpoint discovered CryptXXX version 2.006, an update to CryptXXX, which defeats a Kaspersky Lab decrypter, blocks users' from going online, and locks a user's entire screen, forcing them to log onto a different computer to go online to buy Bitcoin and pay the ransom. The ransomware is distributed via malvertising campaigns, malicious ads on legitimate Web sites, or through an intermediary malware called Bedep.
Source: <http://news.softpedia.com/news/cryptxxx-is-now-undecryptable-prevents-users-from-accessing-their-pc-503884.shtml>

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>

Communications Sector

21. *May 10, Softpedia* – (National) **FTC orders Apple, Google, Microsoft, others to reveal mobile security practices.** The U.S. Federal Trade Commission (FTC) began an investigation May 10 into the security practices at eight major mobile companies including Apple Inc., BlackBerry Limited, Google, Microsoft, and others to determine how the companies plan and carry out security operations for their mobile divisions, and to understand the factors companies consider when deciding whether to patch a vulnerability, among other inquiries. The FTC stated that the investigation is an attempt to understand the current mobile security landscape.
Source: <http://news.softpedia.com/news/ftc-orders-apple-google-microsoft-others-to-reveal-mobile-security-practices-503872.shtml>
22. *May 9, WABC 7 New York City* – (New York) **Time Warner Cable service restored after major outage in New York City area.** Time Warner Cable announced May 9 that Internet, cable TV, and phone service was restored to customers across New York City after multiple fiber optic cables at network providers were cut, leaving customers without service for approximately 7 hours.
Source: <http://abc7ny.com/technology/time-warner-cable-service-restored-after-major-outage-in-new-york-city-area-/1330571/>

For another story, see item [19](#)

Commercial Facilities Sector

23. *May 9, MyNewsLA.com* – (California) **\$4M worth of laptops stolen from Harbor Gateway warehouse.** Los Angeles Police are searching for 5 men suspected of stealing over 7,600 Dell laptop computers worth approximately \$4 million May 6 during an armed robbery at a warehouse in the Harbor Gateway area. The suspects zip-tied a guard and hooked up two trailers containing the merchandise to two trucks before driving off.
Source: <http://mynewsla.com/crime/2016/05/09/4m-worth-of-laptops-stolen-from-harbor-gateway-warehouse/>

Dams Sector

24. *May 10, St. Joseph News-Press* – (Missouri) **City council votes to spend \$3.2 million on levee repairs.** St. Joseph city leaders voted May 9 to appropriate over \$3.2 million in a 4-year project to repair local levees on the Missouri River. The bill serves the purpose of providing funding for and managing construction of river levee system L455 (left bank levee) and R460-471 (right bank levee).
Source: http://www.newspressnow.com/news/local_news/article_e674f788-0f78-5a17-a25b-7938cfd2fc69.html
25. *May 9, KFSN 30 Fresno* – (California) **Crews repair crack in Terminus Dam.** U.S. Army Corps of Engineers officials reported May 9 that crews installed a valve on a 2-inch water line coming from the float well of the Terminus Dam May 8, repairing the

crack and sealing inflow from the exterior of the tower coming in. Crews will continue work to repair another small leak and release water.

Source: <http://abc30.com/news/crews-repair-crack-in-terminus-dam/1330999/>



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.