Daily Open Source Infrastructure Report
22 August 2016

Top Stories

- The FBI is searching August 18 for a man dubbed the "Taxicab Bandit" who is suspected of robbing a BestBank branch in Decatur, Georgia, 2 times since the week of August 8 and other DeKalb County banks. – *Atlanta Journal-Constitution* (See item **1**)
- The U.S. Air Force announced August 18 it awarded a $6.2 million contract to replace its firefighting foam after a report confirmed that drinking water contamination in southern El Paso County, Colorado, may be linked to the firefighting chemicals used at Peterson Air Force Base. – *Associated Press* (See item **22**)
- Researchers discovered that the Locky ransomware reverted to leveraging Microsoft Office documents embedded with malicious macros for distribution to organizations in the health care, telecommunications, and transportations industries. – *SecurityWeek* (See item **26**)
- Eddie Bauer reported August 18 that its point-of-sale (PoS) systems at all 350 locations in the U.S. and Canada were breached after detecting malicious software on its network which may have compromised credit card information. – *Krebs on Security* (See item **28**)

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

Nothing to report

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

1. *August 18, Atlanta Journal-Constitution* – (Georgia) **FBI searching for 'Taxicab Bandit' wanted in bank robberies.** The FBI is searching August 18 for a man dubbed the "Taxicab Bandit" who is suspected of robbing a BestBank branch in Decatur, Georgia, 2 times since the week of August 8 and other DeKalb County banks.
   Source: http://www.ajc.com/news/news/crime-law/fbi-searching-for-taxicab-bandit-wanted-in-bank-ro/nsH3y/

2. *August 18, KCBS 2 Los Angeles* – (California) **'Audi Bandit' sought in string of Bay Area bank robberies.** The FBI is searching August 18 for a man dubbed the "Audi Bandit" who is suspected of robbing at least 3 San Francisco Bay Area banks since May, including a Fremont Bank branch in Livermore and a Wells Fargo Bank branch in Pleasanton in June.
   Source: http://sanfrancisco.cbslocal.com/2016/08/18/audi-bandit-sought-in-string-of-bay-area-bank-robberies/

For another story, see item **28**

Transportation Systems Sector

3. *August 19, Vineland Daily Journal* – (New Jersey) **Blown tire leads to Route 55 shutdown.** All lanes of Route 55 in Vineland, New Jersey, were closed for several hours August 18 while crews worked to clear the wreckage from a 4-vehicle accident that sent 3 people to area hospitals.
   Source: http://www.thedailyjournal.com/story/news/2016/08/19/blown-tire-leads-route-55-shutdown/88994574/

4. *August 19, WNYW 5 New York; Associated Press* – (New Jersey) **1 dead in horrific NJ Transit bus crash.** A New Jersey Transit Corporation bus crashed into another bus in downtown Newark August 19, prompting the closure of Broad Street and Raymond Boulevard for several hours. One driver was killed and 19 passengers were injured.
Source: http://www.fox5ny.com/news/193746749-story

5. *August 19, WTIC 61 Hartford* – (Connecticut) **Serious tractor-trailer accident causes delays on I-91 north in Rocky Hill.** Northbound lanes of Interstate 91 in Rocky Hill, Connecticut, were closed for several hours August 19 while crews worked to clear the wreckage after a semi-truck veered off the road and into a stand of trees. Crews worked for 2 hours to rescue the driver who was trapped inside his vehicle and officials were evaluating a potential fuel spill.
Source: http://fox61.com/2016/08/19/tractor-trailer-accident-causes-delays-on-i-91-north-in-rocky-hill/

6. *August 19, KLTV 7 Tyler* – (Texas) **One dead in wreck on Hwy 155 north of Frankston.** A multi-vehicle crash shut down Highway 155 near Frankston, Texas, for more than 3 hours August 18 while crews worked to clear the wreckage after a semi-truck involved in the crash began leaking fluid on the roadway. One person was killed.
Source: http://www.kltv.com/story/32791564/multi-vehicle-wreck-shuts-down-hwy-155-north-of-frankston

7. *August 18, Washington Post* – (Virginia) **Metro opens police investigation into East Falls Church derailment.** Metro Transit police and two former Federal prosecutors launched an investigation August 18 into whether criminal wrongdoing contributed to the July 29 Silver Line train derailment at the East Falls Church station in Virginia after an investigation by the National Transportation Safety Board and Federal Transit Administration determined the derailment occurred due to degraded rail infrastructure and the failure of Washington Metropolitan Area Transit crews to complete frequent inspections.
Source: https://www.washingtonpost.com/local/trafficandcommuting/metro-opens-criminal-investigation-into-east-falls-church-derailment/2016/08/18/80581080-6571-11e6-8b27-bb8ba39497a2_story.html

8. *August 18, KPCQ 13 Tacoma*– (Washington) **Overturned semi-tanker closes I-5 for hours.** Interstate 5 in Fife, Washington, was closed for nearly 3 hours August 18 while crews worked to clear the scene after a semi-truck overturned and spilled its fuel on the roadway, prompting officials to evacuate nearby buildings as a safety precaution.
Source: http://q13fox.com/2016/08/18/overturned-tanker-truck-leaking-fuel-on-i-5-ramp-near-port-of-tacoma/

9. *August 18, WCPO 9 Cincinnati* – (Ohio) **Washout collapses highway in Highland County** A portion of State Route 785 in Highland County, Ohio, collapsed August 17 following severe storms that swept through the area. Officials said the highway could remain closed for weeks while crews work to repair the damage.

Source: http://www.wcpo.com/news/local-news/highland-county/washout-collapses-highway-in-highland-county

10. *August 18, KABC 7 Los Angeles; Southern California City News Service* – (California) **Crash closes all lanes of PCH in Malibu.** Both directions of Pacific Coast Highway in Malibu, California, were closed for more than 2 hours August 18 while crews worked to clear the wreckage from a 2-vehicle crash involving a semi-truck and another vehicle that left 1 person trapped in their vehicle underneath the semi-truck.
Source: http://abc7.com/traffic/crash-closes-all-lanes-of-pch-in-malibu/1474663/

11. *August 18, WTLV 12 Jacksonville* – (Florida) **I-95 north of downtown reopens after 7 hours.** All lanes of Interstate 95 at the Trout River Bridge in Jacksonville, Florida, were closed for 7 hours August 18 while crews worked to clear the wreckage after a semi-truck jackknifed and overturned, striking 5 other vehicles. One person was sent to an area hospital and HAZMAT crews put down sand to soak up oil and diesel that spilled on the roadway.
Source: http://www.firstcoastnews.com/traffic/traffic-alert-semi-overturns-blocking-i-95-north-of-downtown-jacksonville/301639659

12. *August 18, Tacoma News Tribune* – (Washington) **3-vehicle crash on I-5 in Federal Way adds to traffic woes; backup is 9 miles.** Southbound lanes of Interstate 5 in Federal Way, Washington, were closed for several hours August 18 while crews worked to clear the wreckage from a 3-vehicle accident involving a semi-truck, a motor home, and another vehicle that sent 2 people to area hospitals with injuries.
Source: http://www.thenewstribune.com/news/local/article96470072.html

For another story, see item **26**

Food and Agriculture Sector

Nothing to report

Water and Wastewater Systems Sector

13. *August 18, Associated Press* – (Maryland) **10K gallons of wastewater spill in parkway median.** The Washington Suburban Sanitary Commission notified the Maryland Department of Environment and the Prince George's County Health Department August 18 that more than 10,000 gallons of untreated wastewater spilled from a broken sewer main in a median of the Baltimore-Washington Parkway in Hyattsville, Maryland, August 17. U.S. National Park Service personnel were working to contain the spill and officials were unsure when the repairs would be completed.
Source: https://www.washingtonpost.com/local/10k-gallons-of-wastewater-spill-in-parkway-median/2016/08/18/362dacb4-6566-11e6-b4d8-33e931b5a26d_story.html

14. *August 18, Kalamazoo Gazette* – (Mississippi) **No-contact order for Kalamazoo River lifted days after wastewater plant spill.** Kalamazoo Health and Community Services Department officials canceled a water advisory August 18 after samples of

river water indicated that the portion of the Kalamazoo River affected by a 572,000-gallon partially treated wastewater spill August 16 was safe to enter.
Source: http://www.mlive.com/news/kalamazoo/index.ssf/2016/08/no-contact_order_lifted_for_ka.html

For another story, see item **22**

Healthcare and Public Health Sector

15. *August 18, Associated Press* – (Washington) **Seattle cancer patients likely exposed to tuberculosis by health care worker.** Seattle and King County health officials announced August 18 that about 140 patients at University of Washington Medical Center and Seattle Cancer Care Alliance may have been exposed to tuberculosis after a health care worker employed at the facilities tested positive for the disease. No other staff members have tested positive for tuberculosis.
Source:
http://seattle.cbslocal.com/2016/08/18/seattle-cancer-patients-likely-exposed-to-tuberculosis-by-health-care-worker/

16. *August 18, U.S. Food and Drug Administration* – (National) **Voluntary nationwide recall of Cetylev (Acetylcysteine) effervescent tablets for oral solution due to an inadequate seal of the blister pack.** Arbor Pharmaceuticals, LLC issued a recall August 18 for 3 lots of its Cetylev (acetylcysteine) 500-milligram effervescent tablets due to an inadequate seal of the blister pack. No adverse reactions have been reported and the products were distributed to wholesalers and pharmacies nationwide.
Source:
http://www.fda.gov/Safety/Recalls/ucm517264.htm

17. *August 18, U.S. Food and Drug Administration* – (National) **Sagent Pharmaceuticals initiates a nationwide voluntary recall of Oxacillin for Injection, USP, 10g due to presence of iron oxide particulate matter.** Sagent Pharmaceuticals, Inc. issued a voluntary recall August 18 for its Oxacillin for Injection products manufactured by Astral SteriTech Private Limited due to potential iron oxide contamination after the firm received a complaint stating small, dark particulate matter was found in one vial of the solution. There have been no confirmed reports of adverse reactions and the products were distributed to hospitals, wholesalers, and distributors nationwide.
Source:
http://www.fda.gov/Safety/Recalls/ucm517328.htm

For another story, see item **26**

Government Facilities Sector

18. *August 19, KSBY 6 San Luis Obispo* – (California) **Rey Fire: 600 acres burned, 20% contained, Highway 154 reopened.** Crews reached 20 percent containment August 18 of the 600-acre Rey Fire burning in the Los Padres National Forest in southern Santa Barbara County, California, which has prompted the evacuation of 300 people near the

fire zone and forced the closure of Paradise Road.
Source: http://www.ksby.com/story/32793243/firefighters-responding-to-brush-fire-in-southern-santa-barbara-county

19. *August 19, KSBY 6 San Luis Obispo* – (California) **11,233 acres burned by Chimney Fire, containment increased to 33%.** More than 2,300 fire personnel reached 33 percent containment August 18 of the 11,233-acre Chimney Fire burning near Lake Nacimiento, California, which has destroyed 45 buildings, threatens 232 more, and knocked out power to more than 240 customers. Officials estimated the fire would be contained by August 29.
Source: http://www.ksby.com/story/32788575/chimney-fire-grows-to-8300-acres-near-lake-nacimiento-containment-increased-to-30

20. *August 19, KABC 7 Los Angeles* – (California) **Some evacuations lifted as firefighters make progress on 35,969-acre Blue Cut Fire.** Approximately 1,580 firefighters reached 22 percent containment August 18 of the 35,969-acre Blue Cut Fire burning in San Bernardino County, California, prompting officials to lift evacuation orders for East Oak Hills, South Hesperia, and the West Oak Hills area. Mandatory evacuation orders remained in place for all of Wrightwood, Lytle Creek Canyon, Lone Pine Canyon, Phelan, and West Cajon Valley.
Source: http://abc7.com/news/31600-acre-blue-cut-fire-continues-to-burn-in-cajon-pass;-4%-contained/1474533/

21. *August 18, KTVL 10 Medford* – (Oregon) **Withers Fire reaches 3400 acres, level 1, 2 and 3 evacuations in place.** Crews reached 40 percent containment August 18 of the 3,424-acre Withers Fire burning near Paisley, Oregon, which has prompted officials to issue mandatory evacuation orders for any residences or campers along River Road.
Source: http://ktvl.com/news/local/withers-fire-reaches-2000-acres-level-1-2-and-3-evacuations-in-place

22. *August 18, Associated Press* – (Colorado) **Air Force to change fire foam due to water contamination.** The U.S. Air Force announced August 18 it awarded a $6.2 million contract to replace its firefighting foam with an environmentally friendly foam to reduce the risk of possible contamination of soil and groundwater after a report issued August 17 confirmed that drinking water contamination in southern El Paso County, Colorado, and other sites may be linked to the firefighting chemicals used at Peterson Air Force Base in Colorado Springs. U.S. Air Force officials stated it will replace the foam in fire stations and fire vehicles with the new formula by the end of 2016 after the U.S. Environmental Protection Agency issued stricter guidelines for human exposure to the chemicals, as they have been linked to cancer and other illnesses.
Source: http://gazette.com/us-air-force-to-change-fire-foam-due-to-water-contamination/article/1583128

23. *August 18, KBAK 29 Bakersfield/KBFX 58 Bakersfield* – (California) **More evacuations called for in Cedar Fire, burning more than 9,500 acres.** Crews reached 5 percent containment August 18 of the 9,500-acre Cedar Fire burning near

Alta Sierra in Kern County, California, which has forced the closure of Highway 155 and a portion of Forest Highway 90. Officials issued recommended evacuation orders for Alta Sierra, Slick Rock, and Shirley Meadows in Kern County, as well as for select areas in Tulare County.
Source: http://bakersfieldnow.com/news/local/cedar-fire-continues-to-burn-near-alta-sierra

Emergency Services Sector

Nothing to report

Information Technology Sector

24. *August 18, SecurityWeek* – (International) **Flaws in smart sockets expose networks to remote attacks.** Bitdefender researchers reported a popular brand of smart electrical sockets is plagued with serious vulnerabilities that could be exploited by a remote attacker who knows the media access control (MAC) and default password to take control of the device, make configuration changes, and obtain user information after finding that the socket's hotspot is protected by default credentials and users are not advised to strengthen the credentials, the mobile app transfers Wi-Fi credentials in clear text, which could allow an attacker to intercept the information, and that communications between the device and application go through the manufacturer's server without being encrypted, among other flaws. Researchers stated a patch for the flaws is expected to be released in the third quarter of 2016.
Source: http://www.securityweek.com/flaws-smart-sockets-expose-networks-remote-attacks

25. *August 18, Softpedia* – (International) **Global phishing numbers rise as hosting firms fail to respond.** Cyren released its Cyberthreat Report that analyzed global phishing operations and found that the total number of malicious phishing Universal Resource Locators (URLs) spread on the Internet increased by 14 percent in quarter 2 of 2016 to 4.44 million, and revealed that 20 percent of all phishing pages disappear after 3 hours, with only 40 percent of all pages lasting more than 2 days. The report also states that Google Chrome and Mozilla Firefox are the quickest to identify phishing pages and malicious sites after Chrome detected 73.9 percent of phishing pages within 48 hours and Firefox marked 52.2 percent of the sites.
Source: http://news.softpedia.com/news/global-phishing-numbers-rise-as-hosting-firms-fail-to-respond-507441.shtml

26. *August 18, SecurityWeek* – (International) **Locky ransomware reverts to malicious macros.** FireEye researchers discovered that the Locky ransomware reverted to using Microsoft Office documents embedded with malicious macros to distribute the malware to individuals and organizations in the health care, telecommunications, and transportations industries. Researchers reported that the DOCM files install the ransomware onto a victim's device once the malicious macros are enabled.
Source: http://www.securityweek.com/locky-ransomware-reverts-malicious-macros

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

See item **26**

Commercial Facilities Sector

27. *August 19, WTVC 9 Chattanooga* – (Tennessee) **4-alarm fire guts Soddy Daisy business.** Authorities are investigating the cause of a 4-alarm fire at Norcina Fine Cabinetry in Soddy Daisy, Tennessee, August 19 that caused an estimated $200,000 in damage. HAZMAT crews responded to prevent chemicals from leaking into a nearby creek.
Source: http://newschannel9.com/news/local/4-alarm-fire-guts-soddy-daisy-business

28. *August 18, Krebs on Security* – (International) **Malware infected all Eddie Bauer stores in U.S., Canada.** Eddie Bauer reported August 18 that its point-of-sale (PoS) systems were breached after detecting malicious software on its network which may have compromised credit and debit card information used at more than 350 locations in the U.S. and Canada between January and July 2016. The company removed the malicious software from its PoS systems and stated the breach did not impact purchases made from the company's online store.
Source: http://krebsonsecurity.com/2016/08/malware-infected-all-eddie-bauer-stores-in-u-s-canada/

Dams Sector

Nothing to report

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