Homeland Security

Daily Open Source Infrastructure Report 07 September 2016

Top Stories

- Louisiana officials worked September 5 to secure a Harvest Pipeline Company pipeline after 5,300 gallons of crude oil leaked near Bay Long after a Great Lakes Dredge and Dock Company vessel struck the pipeline during excavation. – *Associated Press* (See item **1**)

- Mazda Motor Corporation issued a recall September 6 for 41,918 of its model years 2009 – 2010 Mazda6 vehicles due to faulty airbag systems that can prevent the airbags from deploying during collisions. – *TheCarConnection.com* (See item **6**)

- About 125,000 gallons of partially treated wastewater spilled into Slocum Creek in Havelock, North Carolina, September 2 after a pump controller at the Havelock Water Plant failed due to heavy rains from Tropical Storm Hermine. – *WNCT 9 Greenville* (See item **21**)

- Two men were arrested in Coweta, Oklahoma, September 2 for their roles in a more than $1 million gift-card theft ring targeting Walmart stores in 31 States. – *Tulsa World* (See item **31**)

Fast Jump Menu

PRODUCTION INDUSTRIES

SUSTENANCE and HEALTH

SERVICE INDUSTRIES

FEDERAL and STATE

Energy Sector

1. *September 6, Associated Press* – (Louisiana) **5,300-gallon oil spill being cleaned in south Louisiana.** The Louisiana Department of Wildlife and Fisheries and the U.S. Coast Guard in New Orleans worked September 5 to secure a Harvest Pipeline Company pipeline after 5,300 gallons of crude oil leaked near Bay Long after a Great Lakes Dredge and Dock Company vessel struck the pipeline during excavation.
   Source: http://www.wdsu.com/news/local-news/new-orleans/5300gallon-oil-spill-being-cleaned-in-south-louisiana/41530734

2. *September 5, WJXT 4 Jacksonville*– (Florida) **Gov. frustrated by slow power restoration.** Crews continued working September 5 to restore power to 33,016 customers in Florida who remained without service after Hurricane Hermine hit the State September 2, prompting the closure of Leon County schools and Florida State University until September 7. Officials reported that 28 State facilities remained without power September 5 and county buildings in Jefferson, Leon, Taylor, and Wakulla counties remained closed.
   Source: http://www.news4jax.com/news/gov-scott-directs-addition-resources-to-help-leon-county-restore-power

3. *September 4, Associated Press* – (Georgia) **36,000 customers still without power in Georgia after Hermine.** Georgia Power officials reported September 4 that approximately 36,000 customers in southeast Georgia remained without power following Tropical Storm Hermine that left nearly 200,000 locations in the Savannah and coastal areas damaged.
   Source: http://www.wctv.tv/content/news/36000-customers-still-without-power-in-Georgia-after-Hermine-392287671.html

4. *September 3, Associated Press* – (South Carolina) **21,000 remain without power as Hermine leaves South Carolina.** Crews worked September 3 to restore service to approximately 21,000 customers across South Carolina who remained without power following Tropical Storm Hermine.
   Source: http://wane.com/2016/09/03/21000-remain-without-power-as-hermine-leaves-south-carolina/

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

5. *September 3, Emporia Gazette* – (Kansas) **Leak at Wolf Creek 'contained, no danger to public.'** Officials from Wolf Creek Nuclear Operating Corporation reported that the Wolf Creek Generating Station in Burlington, Kansas, was manually shutdown September 3 while crews worked to locate and repair a small water leak in the plant's cooling system. Officials did not disclose when the plant would resume power generation.

Source: http://www.emporiagazette.com/area_news/article_e35cb6bc-7134-11e6-b558-6f511d4b9323.html

Critical Manufacturing Sector

6. *September 6, TheCarConnection.com* – (National) **2009-2010 Mazda Mazda6 recalled for airbag problem.** Mazda Motor Corporation issued a recall September 6 for about 41,918 of its model years 2009 – 2010 Mazda6 vehicles sold in the U.S. due to faulty airbag systems caused by poor application of protective coating, which could allow moisture to enter the airbag control unit and cause damage, thereby preventing the airbags from deploying during collisions and increasing the risk of injury.
Source:
http://www.thecarconnection.com/news/1105947_2009-2010-mazda-mazda6-recalled-for-airbag-problem

7. *September 5, Softpedia* – (International) **LuaBot is the first DDoS malware coded in Lua targeting Linux platforms.** Security researchers from MalwareMustDie! discovered a trojan coded in Lua was compromising Linux platforms and internet of things (IoT) devices or Web servers in order to add them as bots inside a larger botnet controlled by the malicious actor. The security researchers reported the LuaBot trojan is packed as an Executable and Linkable Format (ELF) binary targeting Advanced RISC Machines (ARM) platforms and can be found in embedded IoT devices.
Source: http://news.softpedia.com/news/luabot-is-the-first-botnet-malware-coded-in-lua-targeting-linux-platforms-507978.shtml

8. *September 5, Softpedia* – (International) **Mirai DDoS trojan is the next big threat to IoT devices and Linux servers.** MalwareMustDie! (MMD) security researchers discovered a new trojan, dubbed Mirai was targeting Linux servers and internet of things (IoT) devices running Busybox, and a specific set of platforms, including Advanced RISC Machines (ARM) and ARM7, among others, on which IoT devices are built via brute-force attacks on the Telnet port using a list of default admin credentials to exploit cases where users failed to change the built-in passwords. Researchers believe the trojan was built to target digital video recorders (DVRs) and Internet Protocol (IP) cameras.
Source: http://news.softpedia.com/news/mirai-ddos-trojan-is-the-next-big-threat-for-iot-devices-and-linux-servers-507964.shtml

For another story, see item **28**

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

9. *September 2, South Florida Sun-Sentinel* – (Florida) **FBI: Prolific 'Filter Bandit' strikes again at Fort Lauderdale bank.** The FBI is searching September 2 for a man

dubbed the "Filter Bandit" who is suspected of robbing several banks in Broward County, Florida, since August 2014, including an AmTrust Bank branch in Fort Lauderdale September 2.
Source: http://www.sun-sentinel.com/local/broward/fl-fort-lauderdale-filter-bandit-20160902-story.html

For another story, see item **32**

Transportation Systems Sector

10. *September 6, New York Times* – (National) **British Airways computer problems cause widespread delays.** An unexplained computer error disabled British Airways self-service check-in kiosks at multiple international airports, including Chicago O' Hare International Airport, San Francisco International Airport, and Seattle-Tacoma International Airport for several hours September 5 – September 6, causing significant flight delays worldwide. Technicians resolved the error September 6 and officials advised passengers to check in online or via the airline's mobile application before reaching the airport.
Source: http://www.nytimes.com/2016/09/07/business/british-airways-says-computer-problems-cause-widespread-delays.html?_r=1

11. *September 6, WKRN 2 Nashville*– (Tennessee) **Plane makes emergency landing in Nashville after passenger shouts in Arabic, breaks door.** United Airlines Express flight 3550 en route from Cincinnati/Northern Kentucky International Airport to George Bush Intercontinental Airport in Houston was forced to make an emergency landing at Nashville International Airport September 5 after a man broke out of the plane's bathroom and caused a disruption. The man was arrested upon landing and charged with public intoxication and disorderly conduct.
Source: http://wjhl.com/2016/09/06/plane-makes-emergency-landing-in-nashville-after-passenger-shouts-in-arabic-breaks-door/

12. *September 5, WFMY 2 Greensboro* – (North Carolina) **Truck carrying explosive materials overturns in Gaston County.** Officials closed Highway 321 in Gastonia, North Carolina, for several hours September 5 while HAZMAT crews worked to clear the wreckage after a truck carrying ammonium nitrite, fuel oil, and blasting caps overturned. No injuries were reported.
Source: http://www.wfmynews2.com/news/traffic/truck-carrying-explosive-materials-overturns-in-gaston-county/313907018

13. *September 5, KRON 4 San Francisco*– (California) **Shooting on highway causes lane closures in Oakland.** Police closed several lanes of Interstate 880 in Oakland, California, for several hours September 4 while they investigated a shooting between two northbound vehicles near the High Street off-ramp. No injuries were reported and no arrests were made.
Source: http://kron4.com/2016/09/04/shooting-on-highway-causes-lane-closures-in-oakland/

14. *September 5, WCIV 36 Charleston* – (South Carolina) **Crews respond to serious crash with injuries, fatality on Johns Island.** A three-vehicle crash prompted the closure of Main Road at Savannah Highway in Johns Island, South Carolina, for several hours September 5 while crews worked to clear the wreckage. One person was killed.
Source: http://abcnews4.com/news/local/crews-respond-to-serious-crash-with-injuries-on-john-island

15. *September 5, Taft Midway Driller* – (California) **Two children killed in crash on Highway 166.** Highway 166 west of the Cuyama Valley in San Luis Obispo County, California, was closed for nearly 2 hours September 5 while officials investigated the scene of a two-vehicle crash that killed two people and sent five others to an area hospital.
Source: http://www.taftmidwaydriller.com/article/20160905/NEWS/160909864

16. *September 4, Reuters* – (California) **L.A. airport terminal evacuated in second security scare in week.** Terminal 3 at Los Angeles International Airport was evacuated for more than 3 hours September 4 after officials arresting a motorist who was illegally parked outside the terminal sparked a commotion and prompted passengers to rush past a security checkpoint, forcing officials to evacuate the terminal while bomb-sniffing dogs searched the facility. The investigation delayed a total of 18 inbound and outbound flights.
Source: http://www.reuters.com/article/us-usa-security-losangeles-idUSKCN11A14N

17. *September 4, KTVI 2 St. Louis* – (Missouri) **Man struck and killed on I-70 in St. Charles County.** Interstate 70 near O'Fallon, Missouri, was closed for nearly 3 hours September 4 after a pedestrian was fatally struck by a semi-truck while crossing the road.
Source: http://fox2now.com/2016/09/04/i-70-in-st-charles-shut-down-for-accident-reconstruction/

Food and Agriculture Sector

18. *September 2, U.S. Food and Drug Administration* – (National) **Asher's Chocolates/Lewistown, Inc. issues voluntary recall of candy products because of possible health risk.** Asher's Chocolates Lewistown, Inc., a partner of Chester A. Asher Inc., issued a voluntary recall September 2 for its chocolate products sold in 41 variations due to potential Salmonella contamination after routine testing revealed the presence of Salmonella in a single sample. No illnesses have been reported and the products were distributed to retail stores nationwide.
Source:
http://www.fda.gov/Safety/Recalls/ucm519188.htm

19. *September 2, U.S. Food and Drug Administration* – (National) **Wegmans announces voluntary recall for one date code of Wegmans Italian Classics Striped Ricotta & Spinach Ravioli, which may contain pieces of white plastic.** Wegmans Food Markets, Inc. issued a voluntary recall September 2 for approximately 1,638 units of its Wegmans Italian Classics Striped Ricotta & Spinach Ravioli products sold in 9-ounce

packages due to potential contamination with white plastic pieces after customers notified the company that plastic pieces were found in the product. No injuries have been reported and the products were distributed to 90 Wegmans stores in 6 States.
Source:
http://www.fda.gov/Safety/Recalls/ucm519172.htm

20. *September 2, U.S. Food and Drug Administration* – (Hawaii) **Regalo Bakery issues allergy alert on undeclared allergens in bakery products.** Regalo Bakery issued a recall September 2 for six of its products due to undeclared soy, wheat, and artificial food coloring, among other allergens, after a routine Federal inspection revealed the labels failed to declare the presence of the allergens. No illnesses have been reported and the products were distributed to several grocery stores in Hawaii.
Source:
http://www.fda.gov/Safety/Recalls/ucm519169.htm

Water and Wastewater Systems Sector

21. *September 4, WNCT 9 Greenville* – (North Carolina) **125,000 gallons of wastewater discharged in Havelock.** Approximately 125,000 gallons of partially treated wastewater spilled into Slocum Creek in Havelock, North Carolina, September 2 after a pump controller at the Havelock Water Plant failed due to heavy rains from Tropical Storm Hermine. Officials reset the pump controller to prevent further damage.
Source: http://wnct.com/2016/09/04/125000-gallons-of-wastewater-discharged-in-havelock/

Healthcare and Public Health Sector

22. *September 2, WISN 12 Milwaukee* – (Wisconsin) **Medical College of Wisconsin notifies patients of security breach.** The Medical College of Wisconsin (MCW) announced September 2 that approximately 3,200 patients were potentially affected by a security breach after MCW determined that an unauthorized individual used an employee's e-mail account to access the names, addresses, and Social Security numbers, among other personal information, from patient records July 2 – July 4. The company stated it is not aware of any reports of identity theft or fraud related to the incident.
Source:
http://www.wisn.com/news/medical-college-of-wisconsin-notifies-patients-of-security-breach/41491544

Government Facilities Sector

23. *September 5, KDRV 12 Medford* – (California) **Wildfire now nearly 26,000 acres.** About 1,943 firefighters reached 30 percent containment September 5 of the 25,801-acre Gap Fire burning near Happy Camp, California, which prompted officials to issue mandatory evacuation orders for both sides of Highway 96 between Scott River Road and Walker Gulch including Hamburg.
Source:

http://www.kdrv.com/news/GAP_FIRE_UPDATE_Wildfire_Now_Nearly_.html

24. *September 5, Lower Hudson Valley Journal News* – (New York) **Purchase College: Dorm fire wasn't suspicious.** Authorities are investigating the cause of a four-alarm fire at a dormitory at State University of New York at Purchase September 4 that displaced two dozen students. Officials were working to determine the extent of the damages.
Source: http://www.lohud.com/story/news/local/westchester/2016/09/05/suny-purchase-college-fire/89879526/

For another story, see item **2**

Emergency Services Sector

25. *September 5, WCPO 9 Cincinnati* – (Ohio) **Wilmington police: Prisoner in shackles escaped, stole car, still on the loose.** Authorities are searching September 5 for an inmate at Clinton County Jail in Wilmington, Ohio, who escaped police custody during a medical evaluation at Clinton County Memorial Hospital September 4 and stole a vehicle from a nearby home.
Source: http://www.wcpo.com/news/crime/deputies-prisoner-escaped-from-clinton-county-hospital

26. *September 5, KSEE 24 Fresno/KGPE 47 Fresno* – (California) **County jail reopens with new security measures.** Fresno County Jail's main lobby reopened September 4 following a shooting September 3 that left two correctional officers in critical condition. The Fresno County sheriff stated new security measures have been implemented following the incident, including the stationing of an armed deputy and armed correctional officer in the lobby.
Source: http://www.yourcentralvalley.com/news/county-jail-reopens-with-new-security-measures

Information Technology Sector

27. *September 4, SecurityWeek* – (International) **Cerber 3.0 ransomware variant emerges.** TrendMicro researchers reported a new variant of the Cerber ransomware, dubbed Cerber 3.0 emerged as a payload in a malvertising campaign and serves users with a malicious ad in a pop-up window after clicking a video to play, which then redirects the victims to the Magnitude and RIG exploit kits (EKs) landing page. Researchers found the malware appends the .cerber3 extension to the encrypted files, then deletes all copies of the files to prevent users from restoring their files, and prompts victims with a ransom note.
Source: http://www.securityweek.com/cerber-30-ransomware-variant-emerges

28. *September 2, Softpedia* – (International) **Attackers combine three botnets to launch massive DDoS attack.** Sucuri researchers reported attackers combined a home router botnet comprised of 11,767 devices, an internet of things (IoT) closed circuit television (CCTV) botnet comprised of 25,000 cameras, and a botnet made up of compromised

Linux servers to carry out a Layer 7 distributed denial-of-service (DDoS) attack involving traffic from over 47,000 Internet Protocol (IP) addresses. Sucuri stated the 3-botnet distribution enabled the attacker to send 120,000 requests per second without disrupting the operation of the infected machines.
Source: http://news.softpedia.com/news/attackers-combine-three-botnets-to-launch-massive-ddos-attack-507901.shtml

For additional stories, see items **7** and **8**

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 **28**

Commercial Facilities Sector

29. *September 5, Charlotte Observer* – (North Carolina) **Charlotte woman charged with first degree arson in apartment fire.** A Charlotte, North Carolina woman was arrested September 5 after setting fire to an east Charlotte apartment building that displaced 22 residents and caused $100,000 in damage. The American Red Cross was assisting those displaced by the fire and no injuries were reported.
Source: http://www.charlotteobserver.com/news/local/crime/article100045917.html

30. *September 5, Newark Star-Ledger* – (New Jersey) **Newark blaze displaces more than 50 people, officials say.** Authorities are investigating the cause of 4-alarm fire September 5 at a Newark, New Jersey apartment complex that displaced 50 residents and damaged 4 surrounding buildings.
Source:
http://www.nj.com/essex/index.ssf/2016/09/newark_blaze_displaces_more_than_50_people_officia.html

31. *September 4, Tulsa World* – (National) **Coweta police arrest two suspects in nationwide Wal-Mart theft ring.** Two men were arrested in Coweta, Oklahoma, September 2 for their roles in a more than $1 million gift-card theft ring targeting Walmart stores in 31 States where the duo and co-conspirators tricked Wal-Mart employees into loading hundreds of dollars onto reloadable Visa gift cards without paying for the cards. Authorities arrested the duo after store security guards reported the men to the police.
Source: http://www.tulsaworld.com/news/crimewatch/coweta-police-arrest-two-suspects-in-nationwide-wal-mart-theft/article_eff8aa39-8455-54c3-84bd-0b9a29ebea78.html

32. *September 3, Softpedia* – (Tennessee) **Hutton Hotel PoS systems compromised with malware for four years.** Hutton Hotel in Nashville, Tennessee, announced September 2 a security breach may have compromised the payment card information of all customers who used their credit or debit cards at the hotel since September 2012 after discovering that the point-of-sale (PoS) systems at its check-in counter and onsite food and beverage outlets were infected with malware when the hotel's payment processor detected the breach and notified hotel officials.
Source: http://news.softpedia.com/news/hutton-hotels-pos-systems-compromised-with-malware-for-four-years-507924.shtml

Dams Sector

Nothing to report

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

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.