Daily Open Source Infrastructure Report 05 August 2015

Top Stories

- New York officials reported August 3 that the death toll from a Legionnaires' disease outbreak had risen to 7, and that there were a total of 81 reported cases of the disease in the South Bronx area. – *FoxNews.com; Associated Press* (See item **14**)

- California crews reached 12 percent containment August 4 of the 60,000-acre Rocky Fire burning in 3 counties that led to the evacuation of more than 13,000 people. – *CNN* (See item **16**)

- Researchers discovered that the Yahoo! advertising network was hit by a large malvertising attack starting July 28 that leveraged Microsoft Azure Web sites to redirect users to pages hosting the Angler exploit kit to infect systems with ransomware and possibly malware.– *Securityweek* (See item **21**)

- An August 3 fire prompted the evacuation of 125 residents from the Courtyard Apartment Complex in California, and injured two residents. – *KGO 7 San Francisco* (See item **31**)

Fast Jump Menu

PRODUCTION INDUSTRIES

SUSTENANCE and HEALTH

SERVICE INDUSTRIES

FEDERAL and STATE

Energy Sector

1. *August 4, Associated Press* – (Rhode Island; Massachusetts) **More than 100,000 residents without power throughout RI and SE MA.** National Grid reported 109,220 power outages due to severe weather in Rhode Island, as well as 10,000 in Massachusetts August 4. The Massachusetts Bay Transportation Authority (MBTA) also reported a downed tree and an electrical malfunction which delayed MBTA commuter rail service.
   Source: http://wpri.com/2015/08/04/thousands-without-power-throughout-the-state/

2. *August 4, WPIX 11 New York* – (New York) **More than 31,000 customers without power on Long Island.** More than 31,000 PSEG Long Island customers lost power August 4 following severe weather. Crews are unsure when service will be restored.
   Source: http://pix11.com/2015/08/04/more-than-34000-customers-without-power-on-long-island/

3. *August 3, WLWT 5 Cincinnati* – (Ohio) **Giant crater left behind after lightning strikes underground fuel tank.** Emergency crews evacuated a quarter-mile radius around Dixie Gas Depot in Fairfield, Ohio after a lightning strike exploded a 10,000 gallon underground fuel storage tank and compromised 2 others. Crews will investigate the remaining tanks August 4 to determine the extent of the damage.
   Source: http://www.wlwt.com/news/evacuations-underway-in-fairfield-after-lightning-strike-on-dixie-highway/34514750

Chemical Industry Sector

4. *August 3, KFVS 12 Cape Girardeau* – (Illinois) **NRS inspecting Honeywell's Metropolis plant after chemical leak.** The U.S. Nuclear Regulatory Commission is inspecting the Metropolis, Illinois Honeywell plant after a uranium hexafluoride leak caused the facility to be on alert for two hours August 1. The investigation will analyze details of the leak and provide a full report within the next 45 days.
   Source: http://www.kfvs12.com/story/29698319/nrc-inspecting-honeywells-metropolis-plant-after-chemical-leak

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

5. *August 3, Las Vegas Sun* – (Nevada) **Man convicted in Las Vegas mortgage fraud case.** An Arizona man was convicted August 3 for his role in a mortgage fraud scheme in which he and 10 others conspired to cause Federally insured banks about $25 million in losses between 2005 – 2007 by using several investment businesses to recruit straw buyers who obtained mortgage loans for 110 Las Vegas and Henderson homes that they would purchase before going into foreclosure.
   Source: http://lasvegassun.com/news/2015/aug/03/man-convicted-las-vegas-mortgage-fraud-case/

6. *August 3, U.S. Securities and Exchange Commission* – (National) **SEC charges Houston-area businessman in Ponzi scheme.** The U.S. Securities and Exchange Commission charged a co-owner of F.A. Voight & Associates LP and DayStar Funding LP August 3 with allegedly defrauding over 300 investors in a $114 million Ponzi scheme in which he solicited investments towards the development of a "Driver Alertness Detection System" while promising high returns, but instead used funds for Ponzi payments and personal gain funneled to a startup company through 2 other partnership companies.
   Source: http://www.sec.gov/news/pressrelease/2015-158.html

7. *August 3, USA Today* – (International) **Former bank trader convicted in Libor scandal.** A former Citigroup and UBS trader was convicted August 3 of conspiring with two dozen traders and employees to rig the London Interbank Offered Rate (Libor) to benefit their trading positions and boost profits while working for UBS and Citigroup.
   Source: http://www.usatoday.com/story/money/2015/08/03/former-bank-trader-convicted-libor-scandal/31052779/

Transportation Systems Sector

8. *August 4, KTLA 5 Los Angeles* – (California) **210 Freeway partially closed in San Dimas area after big rig crash.** West and eastbound lanes of 210 Freeway through Sand Dimas was shut down August 4 for several hours while crews cleared the scene after a semi-truck overturned and caught on fire. No major injuries were reported.
   Source: http://ktla.com/2015/08/04/multiple-lanes-closed-on-210-freeway-after-big-rig-crashes-in-san-dimas-area/

9. *August 4, WYFF 4 Greenville* – (South Carolina) **All lanes open on I-85 after fiery crash kills one.** All lanes of Interstate 85 in Spartanburg County reopened August 4 after being shut down for several hours August 3 while crews cleared the scene of a fiery crash after a semi-truck overturned and burst into flames. The driver of the semi-truck died at the scene.
   Source: http://www.wyff4.com/news/1-killed-in-fiery-i85-crash-officials-confirm/34511324

10. *August 3, KSTU 13 Salt Lake City* – (Utah) **Diesel spill after semi jack-knifes at I-80,**

I-15 interchange causes road closures. Interstate 80 in Salt Lake City was shut down for several hours August 3 while crews cleared the roadways after a double trailer semi-truck jack-knifed and spilled an unspecified amount of diesel onto the roadway.
Source: http://fox13now.com/2015/08/03/diesel-spill-after-semi-jack-knifes-at-i-80-i-15-interchange-causes-road-closure/

11. *August 3, Associated Press* – (Kentucky) **Officials: 4 injured in plane crash near airport's runway.** Four people were injured in a plane crash in Georgetown, Kentucky, after the plane was forced to make an emergency landing after it lost power August 3.
Source: http://www.wowktv.com/story/29695052/officials-4-injured-in-plane-crash-near-airports-runway

For additional stories, see items **1** and **32**

Food and Agriculture Sector

12. *August 3, U.S. Department of Agriculture* – (Minnesota) **Land O'Frost recalls sausage product due to misbranding.** Land O' Frost, Inc., a Lansing, Illinois establishment, is recalling approximately 17 pounds of Ambassador Beef Summer Sausage products packaged in 12 ounce bags due to an undeclared pork ingredient. The product was produced July 25 and sent to retail stores in Minnesota.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-107-2015-release

Water and Wastewater Systems Sector

13. *August 3, WFMY 2 Greensboro* – (North Carolina) **8,000 Lexington residents will have to boil water.** Almost 8,000 residents are under a boil advisory in Lexington, North Carolina, after crews restored service following a water line break that affected residents, and caused businesses to close for the day August 3.
Source: http://www.wfmynews2.com/story/news/2015/08/03/8000-lexington-residents-will-have-boil-water/31089115/

For another story, see item **14**

Healthcare and Public Health Sector

14. *August 4, FoxNews.com; Associated Press* – (New York) **Death toll in South Bronx Legionnaires' disease outbreak rises to 7, officials say.** Health officials in New York reported August 3 that the death toll from a Legionnaires' disease outbreak had risen to 7, and that there were a total of 81 reported cases of the disease in the South Bronx area. Five cooling towers that returned positive results for the legionella bacteria were decontaminated and authorities continue to investigate the source of the bacteria.
Source: http://www.foxnews.com/health/2015/08/04/death-toll-in-south-bronx-

legionnaires-disease-outbreak-rises-to-7-officials/

15. *August 3, Sioux City Journal* – (National) **Attorney: Dakota Dunes clinic cyber attack affects data for more than 13,000 patients.** Siouxland Pain Clinic in Dakota Dunes notified over 13,000 patients July 31 that their personal and medical information may have been compromised in an attack on the clinic's server that occurred between March 26 and April 2. The clinic was notified of the breach June 26 and continues to investigate the incident.
Source: http://siouxcityjournal.com/news/attorney-dakota-dunes-clinic-cyber-attack-affects-data-for-more/article_d1550c3e-3371-5701-802e-5c90a9b6a9a2.html

Government Facilities Sector

16. *August 4, CNN* – (California) **California wildfires torch 134,000 acres – and counting.** Crews in California reached 12 percent containment August 4 of the 60,000-acre Rocky Fire burning in Lake, Yolo, and Colusa counties that led to evacuation orders for more than 13,000 people. Firefighters worked to contain a total of 21 wildfires in the State that have burned over 134,000 acres collectively.
Source: http://www.cnn.com/2015/08/03/us/california-wildfires/

For another story, see item **18**

Emergency Services Sector

17. *August 4, Bloomington-Normal Pantagraph* – (Illinois) **Governor asks FEMA for storm-related assessment help.** The governor of Illinois issued a State disaster proclamation the week of August 3 for 23 counties that were severely impacted by a series of storms in June and July, and has requested the assistance of the Federal Emergency Management Agency (FEMA) with damage assessments and funding for the counties.
Source: http://www.pantagraph.com/news/local/rauner-asks-fema-for-storm-related-assessment-help/article_a09d31ba-74cc-5676-8210-2020b2fb09a1.html

For another story, see item **16**

Information Technology Sector

18. *August 4, Securityweek* – (International) **Chinese VPN used by APT actors relies on hacked servers.** Security researchers at RSA analyzed a Chinese virtual private network (VPN) service dubbed "Terracotta" and found that the service has at least 31 hacked Windows server nodes worldwide in hospitality, government organizations, universities, technology services providers, and private firms. Researchers have observed compromised servers running the Gh0st Remote Administration Tool (RAT), the Mitozhan trojan, and the Liudoor Backdoor, among others.
Source: http://www.securityweek.com/chinese-vpn-used-apt-actors-relies-hacked-servers

19. *August 4, Help Net Security* – (International) **Macs can be permanently compromised via firmware worm.** Security researchers discovered vulnerabilities in the firmware of Apple computers, dubbed "Thunderstrike 2," in which a worm delivered via a phishing email or malicious Web site could spread across connected devices and systems before rewriting itself in the firmware to ensure persistence. Researchers stated that users need to re-flash the chip that contains the malware in order to get rid of the worm.
Source: http://www.net-security.org/malware_news.php?id=3086

20. *August 4, Softpedia* – (International) **RIG Exploit Kit 3.0 succeeded in infecting 1.25 million machines.** Trustwave researchers reported that version 3.0 of the RIG Exploit Kit (EK) infected an average of 27,000 machines a day, totaling 1.25 million infections, through various campaigns in which it predominantly leveraged Adobe Flash zero-day exploits exposed by a Hacking Team leak in July.
Source: http://news.softpedia.com/news/rig-exploit-kit-3-0-succeeded-in-infecting-1-25-million-machines-488461.shtml

21. *August 4, Securityweek* – (International) **Malvertising hits Yahoo! ad network.** Security researchers at Malwarebytes discovered that the Yahoo! advertising network was hit by a large malvertising attack starting July 28 that leveraged Microsoft Azure Web sites to redirect users to pages hosting the Angler exploit kit (EK) to infect systems with ransomware and possibly banking or ad-fraud malware. The attack was shut down August 3.
Source: http://www.securityweek.com/malvertising-attack-hits-yahoo-ad-network

22. *August 4, Securityweek* – (International) **Zero-day vulnerability in OS X exploited in the wild.** Security researchers from Malwarebytes observed attacks leveraging an unpatched local privilege escalation vulnerability in Apple's OS X operating system (OS) in which an attacker could modify a hidden UNIX file to execute adware and other suspicious software with root permissions.
Source: http://www.securityweek.com/zero-day-vulnerability-os-x-exploited-wild

23. *August 4, Help Net Security* – (International) **79% of companies release apps with known vulnerabilities.** Prevoty released findings from a survey and report on security and application development revealing that many enterprises face challenges in releasing secure software on development schedules, and that 43 percent of respondents admitted to releasing applications with vulnerabilities at least 80 percent of the time, due to business pressures and other concerns.
Source: http://www.net-security.org/secworld.php?id=18702

24. *August 4, Softpedia* – (International) **WordPress 4.2.4 fixes three XSS vulnerabilities and one potential SQL injection.** WordPress released an update for its content management system (CMS) addressing three cross-site scripting (XSS) vulnerabilities, a structured query language (SQL) injection, an issue that allowed attackers to lock posts indefinitely, and a timing side-channel attack vector point in which an attacker could analyze cryptographic algorithm routine execution times.
Source: http://news.softpedia.com/news/wordpress-4-2-4-fixes-three-xss-

vulnerabilities-and-one-potential-sql-injection-488470.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

Nothing to report

Commercial Facilities Sector

25. *August 4, WFLA 8 Tampa* – (Florida) **Evacuations continue this morning in flooded Pasco areas.** Pasco County Fire and Rescue crews reported August 3 that the Oaks View Apartments, Anclote River Estates, and Suncoast Gateway Mobile Home Park in New Port Richey were evacuated due to massive rain flooding that caused safety hazards and electricity to shut down. Officials have issued flood warnings until August 6.
Source: http://wfla.com/2015/08/03/pasco-issues-evacuation-order-in-flood-prone-areas/
Cross-refwater

26. *August 4, WQAD 8 Moline* – (Illinois) **Anchor Lumbar reopens day after fire burns for several hours.** Anchor Lumber of Silvis, Illinois reopened August 4 after an August 3 fire prompted the response of several fire crews to remain on site for over 6 hours extinguishing the flames. The building sustained extensive damage and no injuries were reported.
Source: http://wqad.com/2015/08/03/silvis-building-engulfed-in-flames/

27. *August 4, WVIT 30 New Britain* – (Connecticut) **Lighting might have sparked 3-alarm fire at Groton Condos.** A 3-alarm fire at Kinnesbrook Condos in Groton, Connecticut damaged an apartment unit and displaced residents after lightning stuck the building August 3. No injuries were reported.
Source: http://www.nbcconnecticut.com/news/local/2-Alarm-Fire-at-Groton-Condos-320585702.html

28. *August 4, News Channel 5 Nashville* – (Tennessee) **Woman killed in apartment fire north of Nashville.** Six families were displaced and 1 woman killed after a 2-alarm fire damaged 8 apartment units at the Haynes Garden apartments in Whites Creek Pike, Tennessee August 3. The incident prompted the response of several firefighters to contain the fire.
Source: http://www.scrippsmedia.com/newschannel5/news/Woman-Killed-In-Apartment-Fire-North-Of-Nashville-320583912.html

29. *August 3, Brockton Enterprise* – (Massachusetts) **Stoughton man, 19, charged in IKEA bomb scare.** A Stoughton man was charged August 3 for allegedly making a false bomb threat, falsifying a report, and conducting a wrongdoing after the man fabricated a bomb threat that prompted the evacuation of the building and the response of a State Police Bomb Squad. No injuries were reported.
Source: http://www.enterprisenews.com/article/20150803/NEWS/150809479/?Start=1

30. *August 3, San Diego Union-Tribune* – (California) **Fire damages downtown condo.** An August 3 fire extensively damaged the Park Grove condominiums in San Diego and prompted the evacuations of residents after beginning on the main floor and spreading to surrounding areas. No injuries were reported and damages total $200,000.
Source: http://www.sandiegouniontribune.com/news/2015/aug/03/fire-damages-downtown-condo-electrical/

31. *August 3, KGO 7 San Francisco* – (California) **Apartment fire in Hayward prompts evacuation of 125 residents.** An August 3 fire prompted the evacuation of 125 residents from the Courtyard Apartment Complex after 3 fires, in separate locations, began on the third floor of the building. Two residents were treated for minor injuries and an investigation is ongoing to determine the cause of the fires.
Source: http://abc7news.com/news/apartment-fire-in-hayward-prompts-evacuation-of-125-residents/900054/

32. *August 3, Parsippany-Troy Hills Daily Record* – (New Jersey) **Suspicious boombox prompts Florham Park shopping center evacuation.** Florham Park Police reported that the Florham Park shopping center was evacuated and portions of Columbia Turnpike was closed for 2 hours August 3, after a boombox with a threatening note was left at the Walgreens parking lot. The device was deemed safe and police are looking for the culprit.
Source: http://www.dailyrecord.com/story/news/local/2015/08/03/suspicious-device-shuts-columbia-turnpike-florham-park-cops-say/31056445/

For additional stories, see items **13** and **18**

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.