Daily Open Source Infrastructure Report
29 July 2016

Top Stories

- A former registered broker pleaded guilty July 27 to defrauding ForceField Energy Inc., investors out of $131 million between January 2009 and April 2015 after he and co-conspirators manipulated the price and volume of traded ForceField shares. – *U.S. Attorney's Office, Eastern District of New York* (See item **4**)
- Good Food Concepts, LLC, doing business as Ranch Foods Direct, issued a recall July 26 for approximately 2,606 pounds of its non-intact beef products distributed in Colorado due to potential E.coli O157:H7 contamination. – *U.S. Department of Agriculture* (See item **8**)
- Crews reached 10 percent containment July 27 of the Soberanes Fire which has burned over 23,500 acres, threatens 2,000 structures, and has destroyed 34 homes and 10 outbuildings in California. – *Reuters* (See item **13**)
- The U.S. President's administration released Presidential Policy Directive/PPD-41 July 26 detailing the U.S. Cyber Incident Coordination, setting forth principles that govern the Federal Government's response to cyber incidents. – *Whitehouse.gov* (See item **19**)

Fast Jump Menu

Energy Sector

1. *July 28, Arizona Daily Star* – (Arizona) **Thousands without power in metropolitan Tucson.** Tucson Electric Power Co. crews worked July 28 to restore power to approximately 12,000 customers who remained without service following severe storms July 27 that knocked out electricity to more than 21,000 customers.
   Source: http://tucson.com/news/local/thousands-without-power-in-metropolitan-tucson/article_ca46dcde-5465-11e6-b56c-9728034e5fe2.html

2. *July 28, Riverside Press-Enterprise* – (California) **ENERGY: Statewide flex alert extended by 1 day.** The California Independent System Operator issued a Flex Alert July 27 **–** July 28, asking residents to cut down and conserve energy during peak hours due to high temperatures in the State which puts the State's power grid under stress.
   Source: http://www.pe.com/articles/stress-809205-landed-surrounding.html

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

3. *July 27, SecurityWeek* – (International) **PayPal abused in banking trojan distribution campaign.** Proofpoint security researchers discovered malicious actors were distributing the Chthonic banking trojan, a variant of the Zeus malware, via legitimate-looking PayPal emails to request money from users by sending money request messages claiming an illicit $100 transfer was made to the victim's account which could be returned by clicking the malicious Goo.gl link that redirects the user to "katyaflash[.]com/pp.php," where the malware is downloaded onto the device in the form of an obfuscated JavaScript file that connects to the command and control (C&C) server. Researchers discovered the malware was also downloading a previously undocumented second-stage payload dubbed AZORult.
   Source: http://www.securityweek.com/paypal-abused-banking-trojan-distribution-campaign

4. *July 27, U.S. Attorney's Office, Eastern District of New York* – (National) **Registered**

broker pleads guilty to securities fraud for participating in a $131 million market manipulation scheme. A former registered broker pleaded guilty July 27 to defrauding ForceField Energy Inc., investors out of $131 million between January 2009 and April 2015 after he and co-conspirators manipulated the price and volume of traded ForceField shares by orchestrating the trading of ForceField stock to create the appearance of interest and trading volume in the stock, and concealing payments to stock promoters and broker dealers who claimed to be independent of the company, among other fraudulent means. The charges also state that a ForceField executive paid kickbacks to the broker in exchange for purchasing company stocks in his client's brokerage accounts between October 2014 and April 2015.
Source: https://www.justice.gov/usao-edny/pr/registered-broker-pleads-guilty-securities-fraud-particpating-131-million-market

Transportation Systems Sector

5. *July 28, Terre-Haute Tribune-Star* – (Indiana) **Two men remain hospitalized following tractor, truck crash on US 36.** A 2-vehicle crash left 2 men severely injured and closed U.S. 36 in Parke County for more than 6 hours July 27.
Source: http://www.tribstar.com/news/update-farm-tractor-semi-truck-involved-in-u-s-crash/article_0f33caf4-5430-11e6-9cf6-7b669dww6fe59e.html

6. *July 28, Hartford Courant* – (Connecticut) **Serious crash on I-84 west in Southington; highway closed.** Westbound lanes of Interstate 84 in Southington, Connecticut, were closed for more than 2 hours July 28 due to an accident involving 2 vehicles that left 2 people injured.
Source: http://www.courant.com/breaking-news/hc-southington-crash-0729-20160728-story.html

7. *July 27, Fort Morgan Times* – (Colorado) **Semi crash shuts down highway.** Interstate 76 near mile marker 80 in Colorado was closed for nearly 5 hours July 27 while crews worked to clear the wreckage from a 2-vehicle crash involving 2 semi-trucks that sent both drivers to an area hospital with minor injuries.
Source: http://www.fortmorgantimes.com/fort-morgan-local-news/ci_30177377/semi-crash-shuts-down-highway

For another story, see item **14**

Food and Agriculture Sector

8. *July 27, U.S. Department of Agriculture* – (Colorado) **Good Food Concepts, LLC D.B.A. Ranch Foods Direct recalls non-intact beef products due to possible E.coli O157:H7 contamination.** Good Food Concepts, LLC, doing business as Ranch Foods Direct, issued a recall July 26 for approximately 2,606 pounds of its non-intact beef products sold in 25 variations due to potential E.coli O157:H7 contamination after Federal health officials discovered a potential link between the beef products and an E.coli O157:H7 illness outbreak in Colorado. The products were distributed to wholesale and retail locations in Colorado.

Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-064-2016-release

9. *July 27, U.S. Department of Labor* – (Florida) **OSHA cites Pilgrim's Pride for medical mismanagement, fall, machine guarding and other safety, health hazards; proposes $78K in fines.** The Occupational Safety and Health Administration cited Pilgrim's Pride Corp., with 14 serious and 8 other-than-serious safety and health violations July 25 following an investigation at the Live Oak, Florida facility which revealed that the company failed to ensure workers followed energy-control procedures to prevent unexpected machine start-ups, exposed workers to amputation hazards, and failed to make timely medical referrals for workplace injuries, among other violations. Proposed penalties total $78,175.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=32841

10. *July 27, U.S. Department of Agriculture* – (National) **The TDL Group Corp., recalls dried chicken soup mix products distributed without benefit of import inspection.** The TDL Group Corp., issued a recall July 27 for approximately 636 pounds of its "Tim Hortons Chicken Noodle Soup Mix" products sold in 16.9-ounce packages after a Federal import inspector discovered the products were not presented for inspection when entering the U.S. during routine monitoring activities. There have been no confirmed reports of adverse reactions and the products were shipped to restaurants in Maine, New Jersey, New York, and Pennsylvania.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-066-2016-release

Water and Wastewater Systems Sector

11. *July 28, WNCT 9 Greenville* – (North Carolina) **1,500 gallons of wastewater spilled in Mill Creek.** City officials are testing the water after about 1,500 gallons of wastewater spilled in Mill Creek in the city of Jacksonville, North Carolina, July 27 when a pipe broke in the Northwoods neighborhood. The spill was contained and authorities reported that there is no ongoing threat to the environment.
Source: http://wnct.com/2016/07/27/1500-gallons-of-wastewater-spilled-in-mill-creek/

Healthcare and Public Health Sector

12. *July 28, U.S. Food and Drug Administration* – (National) **FDA approves Adlyxin to treat type 2 diabetes.** The U.S. Food and Drug Administration approved Adlyxin, a once-daily injection to improve blood sugar levels in adults with type 2 diabetes July 28.
Source: http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm513602.htm

Government Facilities Sector

13. *July 28, Reuters* – (California) **Central California wildfire destroys 34 homes, forces 350 to evacuate.** Crews reached 10 percent containment of the Soberanes Fire July 27 which has burned over 23,500 acres, threatens 2,000 structures, and has destroyed 34 homes and 10 outbuildings between Big Sur and the town of Carmel-by-the-Sea. Approximately 3,000 firefighters in the State reached 40 percent containment of the 38,350-acre Sand Fire burning in the Angeles National Forest.
Source: http://www.reuters.com/article/us-california-fire-idUSKCN10816V

14. *July 28, Idaho Statesman* – (Idaho) **Fire managers warn drones could shut down flights near Idaho City.** Crews worked July 28 to contain the 12,986-acre Pioneer Fire burning in the Boise National Forest in Idaho. The fire prompted the closure of Highway 21 from mile marker 48 to mile marker 72.5, and threatens at least 10 structures.
Source:
http://www.idahostatesman.com/news/local/environment/fires/article92120957.html

Emergency Services Sector

15. *July 27, Associated Press* – (Oklahoma) **AT&T: Oklahoma's 911 emergency telephone service restored.** AT&T Inc., reported that emergency 9-1-1 service was restored after call routing was impacted for approximately 2 hours July 27 in portions of Oklahoma. The company is investigating the source of the outage, which involved a power issue at a facility in the Oklahoma City area.
Source: http://newsok.com/article/5511348

Information Technology Sector

16. *July 28, SecurityWeek* – (International) **Many web attacks come from United States: Sucuri.** Researchers at Sucuri analyzed metadata from 30 days of Web traffic and blocked requests from its firewall product and found that the Structured Query Language (SQL) injection, brute force, and other exploit attempts had various browser user agents, more than one-third of the attacks came from the U.S. followed by Indonesia and China, and that when it came to operating systems (OS) 45 percent of attacks came from Microsoft Windows.
Source: http://www.securityweek.com/many-web-attacks-come-united-states-sucuri

17. *July 28, Help Net Security* – (International) **Media-stealing Android app targets developers.** Google removed the "HTML Source Code Viewer" app from its Google Play distribution service after Symantec researchers discovered the malicious app stole photos and videos from victims' mobile devices by requesting permissions to access the device's external storage. The app targeted all versions of Android after and including Gingerbread.
Source: https://www.helpnetsecurity.com/2016/07/28/media-stealing-android-app/

18. *July 28, Softpedia* – (International) **Chrome, Firefox vulnerable to crashes via search**

suggestions. Nightwatch Cybersecurity researchers found that Google Chromium, Android, and Mozilla Firefox do not protect browser built-in search suggestions via an encrypted Hypertext Transfer Protocol Secure (HTTPS) channel, which could allow an attacker on the local channel to intercept search suggestion inquiries and answer before the search provider. Firefox, Chrome, and Android are working to address the issue.
Source: http://news.softpedia.com/news/chrome-firefox-vulnerable-to-crashes-via-search-suggestions-506722.shtml

19. *July 26, Whitehouse.gov*– (National) **Presidential Policy Directive – United States Cyber Incident Coordination.** The U.S. President's administration released Presidential Policy Directive/PPD-41 July 26 detailing the U.S. Cyber Incident Coordination, which sets forth principles that govern the Federal Government's response to cyber incidents and the designation of responsibility to certain Federal agencies, including the FBI and DHS.
Source: https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

For another story, see item **3**

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 **15**

Commercial Facilities Sector

20. *July 27, KMOV 4 St. Louis* – (Missouri) **Crews respond to 4-alarm fire at De Soto storage facility overnight.** Authorities are investigating the cause of a 4-alarm fire at the Budget Self-Storage facility in De Soto, Missouri, July 26 – July 27 that caused external or internal damage to 32 units. No injuries were reported.
Source: http://www.kmov.com/story/32550398/crews-respond-to-4-alarm-fire-at-desoto-storage-facility-overnight

21. *July 26, WPVI 6 Philadelphia* – (Pennsylvania) **Smoke forces evacuations at Montgomery Mall.** The Montgomery Mall in Montgomery Township, Pennsylvania, was evacuated for approximately 2 hours July 26 after a power outage caused a generator to malfunction, releasing an electrical odor and smoke into the shopping center. No injuries were reported.
Source: http://6abc.com/news/fire-forces-evacuations-at-montgomery-mall/1443442/

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