Daily Open Source Infrastructure Report
04 August 2014

Top Stories

- A 12-inch water main ruptured in Hyattsville, Maryland, July 31 sending an estimated 6 million gallons of water gushing onto Route 1 and prompting a closure of the roadway through August 2 for repairs. – *WJLA 7 Washington, D.C.* (See item **16**)
- A boil water advisory was issued to roughly 5,000 residents in the Village of Ossining, New York, through August 3 after a water main break July 31 that left the water supply open to contamination. – *WABC 7 New York City* (See item **17**)
- Authorities charged a DCM Erectors Inc. official July 31 with defrauding a government program of millions of dollars during work performed for the Port Authority of New York and New Jersey in the redevelopment of the World Trade Center. – *Reuters* (See item **20**)
- Researchers from SRLabs reported developing a new piece of malware that can reprogram USB controller chips to spoof other devices, allowing an attacker to take control of a computer, steal data, and perform other actions. – *Securityweek* (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. *July 31, U.S. Department of Labor* – (New York) **Explosion at Tonawanda Coke Corp. results in serious safety violations and $161,100 in US Department of Labor OSHA fines.** Tonawanda Coke Corp., and Kirchner LLC were issued 15 serious and 2 repeat violations from the Occupational Safety and Health Administration July 31 following a January 31 explosion at its River Road plant in New York that injured 3 workers and damaged electrical equipment. Proposed fines totaled $161,100.
   Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=26457

For additional stories, see items **2**, **9**, and **18**

[Return to top]

Chemical Industry Sector

2. *July 31, Enid News and Eagle*– (Oklahoma) **Up to 20,000 gallons of hydrochloric acid spilled near Hennessey.** Between 350 and 500 barrels of hydrochloric acid spilled into an alfalfa field at a Blake Production Co. oil well site in Hennessey July 28 when a tank holding up to 20,000 gallons of the fracking chemical began leaking. Crews immediately spread soda ash on the spill to counteract the acid and a contractor was hired to aid with the environmental cleanup associated with the release.
   Source: http://www.enidnews.com/featuredstory/x197378238/Fracking-spill-dumps-480-barrels-of-HCL-acid-SW-of-Hennessey

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

3. *July 31, U.S. Department of Labor* – (Ohio) **Major Metals Co. cited by US Department of Labor's OSHA for exposing workers to amputation and other serious hazards.** The Occupational Safety and Health Administration cited steel tubing manufacturer Major Metals Co., with 10 serious safety violations at its Mansfield, Ohio facility for failing to protect workers from amputation, fall, and other hazards. Proposed fines totaled $41,300.
   Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=26463

[Return to top]

Defense Industrial Base Sector

See item 25

[Return to top]

Financial Services Sector

4. *August 1, Softpedia* – (International) **New point-of-sale malware "Backoff" scrapes RAM for card data.** The U.S. Computer Emergency Response Team (US CERT) published an advisory warning of a new family of malware known as "Backoff" that can compromise point-of-sale (PoS) systems by compromising remote desktop applications and then performing memory scraping to obtain payment card track data. The malware currently has very low rates of detection in most antivirus engines and contains various other capabilities including keystroke logging and injecting a malicious stub into explorer.exe to increase persistency.
   Source: http://news.softpedia.com/news/New-Point-of-Sale-Malware-Backoff-Scrapes-RAM-For-Card-Data-453051.shtml

5. *July 31, Krebs on Security* – (National) **Sandwich chain Jimmy John's investigating breach claims.** Sandwich restaurant chain Jimmy John's reported that it is working with authorities to investigate a possible breach of customer payment data.
   Source: https://krebsonsecurity.com/2014/07/sandwich-chain-jimmy-johns-investigating-breach-claims/

6. *July 31, KUSA 9 Denver* – (Colorado) **'Good Grammar Bandit' bank robber strikes again.** The FBI believes that a suspect known as the "Good Grammar Bandit" was responsible for the robbery of a Chase Bank branch in Thornton July 29, the seventh robbery in the Denver area linked to the suspect.
   Source: http://www.wfmynews2.com/story/news/crime/2014/07/31/good-grammar-bandit/13442831/

[Return to top]

Transportation Systems Sector

7. *August 1, Associated Press* – (Indiana) **Semi crash coats Indianapolis highway in butter.** Eastbound lanes of Interstate 465 in Indianapolis were closed for several hours August 1 for cleanup after a semi-truck overturned spilling about 45,000 pounds of packages of butter and other dairy products. Police reported that the driver fell asleep and hit a highway barrier.
   Source: http://www.washingtontimes.com/news/2014/aug/1/semi-crash-coats-i-465-lanes-with-spilled-butter/

8. *August 1, WAFB 9 Baton Rouge* – (Louisiana) **Train derailment causes heavy traffic**

delays, no spills, evacuations called off. Seven cars carrying chemicals, lubricant oil, and silica pellets derailed from a 105-car Canadian National train in Baton Rouge August 1 closing nearby roadways for approximately 2 hours while authorities investigated the derailment.
Source: http://www.wafb.com/story/26172799/train-derailment-causes-heavy-traffic-delays-evacuations

9. *July 31, KOB 4 Albuquerque* – (New Mexico) **One dead after oil field pipeline explosion south of Artesia.** A worker was killed in a Diversified Oil Field Services-owned oil field explosion near Artesia July 30 while working in a pit cutting pipeline and disassembling PVC pipe. The pipeline exploded, trapping the worker inside the pit while three others escaped.
Source: http://www.kob.com/article/stories/S3520869.shtml

10. *July 31, Associated Press* – (Maryland) **NTSB: Cracked rail caused 2012 coal train derailment that killed 2 in Maryland.** The National Transportation Safety Board released a report July 31 concluding its investigation into a 2012 CSX train derailment in Ellicott City that killed two individuals and found that the section of the rail that caused the derailment showed evidence of gradual breakdown, which CSX was aware of during inspections it conducted every 30 days. The area of the track where the derailment occurred had been scheduled for an overhaul and CSX has since installed a fence to keep people off the bridge.
Source:
http://www.tribtown.com/view/story/70f8664e0c724bfda147237ba9552d6c/MD--Fatal-Train-Derailment

[Return to top]

Food and Agriculture Sector

11. *July 31, Associated Press* – (Illinois) **Man accused of putting needles in packaged meat.** Authorities arrested July 31 an Illinois man accused of tampering with packaged meat and inserting sewing needles into products within the meat section of a Shop 'n Save grocery store in Belleville at least seven times since May 2013. A company representative stated that customers who purchased meat products at the store prior to July 12 should not consume the products and that the issue was believed to be exclusive to the Belleville location.
Source: http://news.msn.com/crime-justice/man-accused-of-putting-needles-in-packaged-meat

12. *July 31, Reuters* – (National) **U.S. CDC says salmonella outbreak from Foster Farms' chicken appears over.** Representatives from the U.S. Centers for Disease Control and Prevention stated July 31 that a Salmonella Heidelberg outbreak linked to contaminated Foster Farms' chicken appears to be over after sickening 634 individuals in 29 States and Puerto Rico since March 2013. The officials also reported that scientists identified seven strains of the bacteria in the outbreak and 38 percent of the sickened individuals were hospitalized.

Source: http://www.reuters.com/article/2014/07/31/us-usa-chicken-salmonella-fosterfarms-idUSKBN0G02QX20140731

13. *July 31, Food Safety News* – (National) **California firm recalls jarred food products for botulism risk.** VR Green Farms voluntarily issued a recall for a variety of its jarred food products sold at the VR Green Farms stand in San Clemente, California, and via nationwide Internet sales due to possible Clostridium botulinum contamination. California and Ohio health officials are working with the U.S. Food and Drug Administration in the investigation of two cases of suspected foodborne infections that are possibly connected to the company's Pine Nut Basil Pesto product.
Source: http://www.foodsafetynews.com/2014/07/consumers-warned-of-ca-jarred-food-products-due-to-botulism-risk

14. *July 30, Food Poisoning Bulletin* – (International) **Pumpkin seeds recalled for undeclared sulfites.** New York-based Starway Incorporated issued a recall for 12-ounce packages of Peony Mark Brand Roasted and Salted Pumpkin Seeds due to undeclared sulfites. The product was imported from China and distributed throughout the U.S.
Source: http://foodpoisoningbulletin.com/2014/pumpkin-seeds-recalled-for-undeclared-sulfites/

15. *July 29, U.S. Food and Drug Administration* – (National) **Natural Grocers by Vitamin Cottage issues voluntary recall for various Chunks of Energy products because they contain Organic Carob Powder from Ciranda, Inc., which may be contaminated with Salmonella.** Natural Grocers issued a recall for its Chunks of Energy Carob Greens and Chunks of Energy Data/Flax/Tumeric products because they were manufactured using organic carob powder from Ciranda, Inc., which may be contaminated with Salmonella. The products were sold in small bags in the refrigerated bulk foods section of 84 Natural Grocer's stores.
Source: http://www.fda.gov/Safety/Recalls/ucm407197.htm

For additional stories, see items 5 and 7

[Return to top]

Water and Wastewater Systems Sector

16. *August 1, WJLA 7 Washington, D.C.* – (Maryland) **Huge water main break floods major Hyattsville road with 6 million gallons.** A 12-inch water main ruptured in Hyattsville, Maryland, July 31 causing the road to buckle and sending an estimated 6 million gallons of water gushing onto Route 1. About 30 homes and businesses were without water as crews worked to repair the pipe closing a stretch of Rhode Island Avenue through the weekend of August 2.
Source: http://www.wjla.com/articles/2014/07/huge-water-main-break-floods-roadway-in-hyattsville-md--105636.html

17. *August 1, WABC 7 New York City* – (New York) **Boil water advisory issued in**

Ossining after water main break. A boil water advisory was issued to roughly 5,000 residents in the Village of Ossining through August 3 after a water main break July 31 that left the water supply open to contamination.
Source: http://7online.com/health/boil-water-advisory-issued-in-ossining/232302/

18. *July 31, KCRA 3 Sacramento* – (California) **Fire at Modesto Irrigation District substation burns out.** A July 31 fire at the Modesto Irrigation District substation plant in California was out several hours after it ignited after crews decided to let the blaze burn out on its own. Authorities are investigating the cause of the fire and are assessing the total amount of damage.
Source: http://www.kcra.com/news/local-news/news-modesto/fire-ignites-at-modesto-irrigation-district-substation/27242886

[Return to top]

Healthcare and Public Health Sector

Nothing to report

[Return to top]

Government Facilities Sector

19. *August 1, KRCR 7 Redding* – (California) **New evacuations issued for Day Fire.** Crews reached 5 percent containment August 1 of the 7,000-acre 3-7 Day Fire in Modoc County prompting the mandatory evacuation of residents between Schneider Ranch Road to the end of Day Road, the Lookout area, and the Lookout Big Valley Ranchettes, while 200 structures remained threatened.
Source: http://www.krcrtv.com/news/local/new-evacuation-advisory-issued-for-37-day-fire/27261624

20. *July 31, Reuters* – (New York) **World Trade Center contractor charged in multimillion-dollar fraud.** The chief executive of DCM Erectors Inc., was charged by federal authorities July 31 with defrauding a government program intended to promote minority-and women-owned businesses during work performed for the Port Authority of New York and New Jersey in the redevelopment of the World Trade Center. The chief executive allegedly paid the owners of two contracting businesses to aid him in falsifying documents made to appear as though they had done work for the company.
Source: http://www.reuters.com/article/2014/07/31/us-usa-crime-worldtradecenter-idUSKBN0G02ST20140731

21. *July 31, Dallas Morning News* – (Texas) **Arlington police, fire investigating white-powder letter handled by 3 workers at municipal courthouse.** The Municipal Court building in Arlington, Texas, was on lock down while authorities investigated a white-powder letter sent to the building July 31. Three mailroom workers who handled the letter were isolated while officials tested the package which they believe was harmless.
Source: http://thescoopblog.dallasnews.com/2014/07/arlington-police-fire-

investigating-white-powder-letter-handled-by-3-workers-at-municipal-courthouse.html/

For another story, see item **22**

[Return to top]

Emergency Services Sector

22. *July 31, McAlester News-Capital* – (Oklahoma) **Heavy rains knocks out sheriff's phones, flood emergency management offices.** Regular phone lines for the Pittsburg County Sheriff's Office and the Office of Emergency Management (OEM) were down July 31 while the OEM was flooded due to heavy rains. City crews pumped out manhole covers while parts of the Pittsburg County Election Board Office were also flooded.
    Source: http://www.mcalesternews.com/local/x1849845297/Heavy-rains-knocks-out-sheriffs-phones-flood-emergency-management-offices

[Return to top]

Information Technology Sector

23. *August 1, Securityweek* – (International) **USB device firmware can be reprogrammed to hide sophisticated malware.** Researchers from SRLabs reported developing a new piece of malware that can reprogram USB controller chips to spoof other devices, allowing an attacker to take control of a computer, steal data, and perform other actions. The researchers plan to demonstrate the "BadUSB" malware at the upcoming Black Hat security conference.
    Source: http://www.securityweek.com/usb-device-firmware-can-be-reprogrammed-hide-sophisticated-malware

24. *August 1, Softpedia* – (International) **Hackers steal video game source code.** Dell SecureWorks' Counter Threat Unit identified a group of attackers labeled Threat Group-3279 that has been observed targeting video game and entertainment companies to steal source code and create cracks or cheat codes for games. The group is believed to be associated with the China Cracking Group and leverages a variety of tools and pieces of malware, including ones created by the group.
    Source: http://news.softpedia.com/news/Hackers-Steal-Video-Game-Source-Code-453108.shtml

25. *August 1, Securityweek* – (International) **"Pitty Tiger" threat actors possibly active since 2008: FireEye.** Researchers at FireEye analyzed the "Pitty Tiger" advanced persistent threat group first identified by Airbus Defense & Space and found that the group may have been active since 2008. The Pitty Tiger campaign targeted a variety of sectors including the defense and telecoms industries, and is believed to be operating from China.
    Source: http://www.securityweek.com/pitty-tiger-threat-actors-possibly-active-2008-fireeye

26. *August 1, Securityweek* – (International) **New ransomware uses GnuPG to encrypt files.** Researchers at Symantec and Trend Micro analyzed a new piece of ransomware dubbed Trojan.Ransomcrypt.L or BAT_CRYPTOR.A that uses GNU Privacy Guard to encrypt files for ransom and can be easily updated by its controllers. Trend Micro also identified another new piece of ransomware dubbed Cryptoblocker which does not use RSA keys and appears to have been written by inexperienced writers.
Source: http://www.securityweek.com/new-ransomware-uses-gnupg-encrypt-files

27. *August 1, Softpedia* – (International) **Fiesta Exploit Kit delivers double payload.** A Malwarebytes researcher reported that attackers have modified the way the Fiesta Exploit Kit delivers its malicious payload by delivering two malicious files at once to attempt to avoid antivirus detection for at least one file.
Source: http://news.softpedia.com/news/Fiesta-Exploit-Kit-Delivers-Double-Payload-453143.shtml

For another story, see item **4**

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

[Return to top]

Communications Sector

28. *July 31, U.S. Department of Labor* – (West Virginia) **Cell tower company cited by OSHA for safety hazards following fatality in Clarksburg, West Virginia, tower collapse in February 2014.** Oklahoma-based S and S Communication Specialists Inc., was cited for two serious safety violations July 31 by the Occupational Safety and Health Administration following the February collapse of a communication tower in Clarksburg that killed two employees and a firefighter and injured two others. Proposed fines totaled $7,000.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=26472

For another story, see item **25**

[Return to top]

Commercial Facilities Sector

29. *August 1, WJXT 4 Jacksonville* – (Florida) **Water slide collapses at Clay Co.**

community pool. Thirteen Fleming Island High School students were injured when a water slide partially collapsed into a retention pond at the Eagle Harbor Community Pool in Clay County July 31 after more than the allowed amount of occupants gathered on the stairs leading to the slide during a school-sponsored party.
Source: http://www.news4jax.com/news/water-slide-collapses-at-clay-county-community-pool-witnesses-say/27255370

30. *August 1, Munster Times* – (Indiana) **22 families displaced by stubborn fire at Highland apartment building.** Dozens of residents were displaced from 22 units of the Porte De L'eau apartment complex in Highland, Illinois, after the structure suffered severe damage from a 3-alarm fire July 31. The cause of the blaze is under investigation.
Source: http://www.nwitimes.com/news/local/lake/highland/families-displaced-by-stubborn-fire-at-highland-apartment-building/article_e3ade4d5-bcf8-5085-a974-352130de75b5.html

31. *July 31, Chicago Tribune* – (Illinois) **Police: Gunman and victim in Loop shooting 'had been friends for years'.** An ArrowStream employee that was allegedly disgruntled about a recent demotion shot and wounded the company's CEO before fatally shooting himself July 31 inside the Bank of America office building in the financial district of Chicago. Police secured the building and tenants were instructed to stay in place while authorities investigated the incident.
Source: http://www.chicagotribune.com/news/local/breaking/chi-police-responding-to-shooting-in-loop-20140731-story.html

32. *July 31, WCBS 2 New York City* – (New York) **3 hurt after glass falls from Midtown Manhattan building.** At last three individuals were injured July 31 when 50 to 60 pounds of glass fell from the 18th floor of a commercial building onto a crowded sidewalk in the Midtown area of New York City after a piece of machinery used during renovation work bumped into the glass pane causing it to shatter. The New York City Department of Buildings is investigating the incident.
Source: http://newyork.cbslocal.com/2014/07/31/glass-falls-from-57th-street-building/

For another story, see item **16**

[Return to top]

Dams Sector

Nothing to report

[Return to top]

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.