Daily Open Source Infrastructure Report
15 January 2014

Top Stories

- Researchers found that the Icefog cyberespionage campaign that targeted defense and technology companies in September 2013 also compromised the systems of three U.S. oil and gas companies. – *Threatpost* (See item **1**)
- A 48-inch water main that broke January 13 and flooded a shopping center in Philadelphia lost around 13 million gallons of water and caused at least $3 million in damage. – *Philadelphia Inquirer* (See item **15**)
- Roswell, New Mexico police arrested a suspect January 14 following a shooting at Berrendo Middle School that left two people critically injured. – *USA Today; Associated Press* (See item **19**)
- One person was fatally shot and another was wounded after an altercation erupted at the Grove 16 Theatre in Wesley Chapel, Florida, January 13. – *NBC News* (See item **30**)

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. *January 14, Threatpost* – (International) **Java version of Icefog espionage campaign hit 3 US oil, gas companies.** Kaspersky Lab researchers found that the Icefog cyberespionage campaign that targeted defense and technology companies in Japan and South Korea and that was revealed in September 2013 also compromised the systems of three U.S. oil and gas companies using a Java version of the campaign. The companies were notified of the infection and two had removed the malware from their systems by January 14.
   Source: http://threatpost.com/java-version-of-icefog-espionage-campaign-hit-3-us-oil-gas-companies/103567

2. *January 13, Shreveport Times* – (Louisiana) **4 arrested in $200,000 copper wire theft.** Authorities are still searching for a fifth person involved in a 2013 theft of more than $200,000 in copper wire from the Dolet Hills Lignite Mine operations in Mansfield, Louisiana. Police arrested and charged four other men connected to the theft.
   Source: http://www.shreveporttimes.com/article/20140113/NEWS01/301130028/4-arrested-in-200-000-copper-wire-theft

3. *January 13, Associated Press* – (Kansas) **Gasoline leaks at Kansas City fuel distribution center.** A fuel leak which occurred at a valve connected to an above-ground storage tank at the Magellan Midstream Partners petroleum terminal in Kansas City, Kansas, caused 100 barrels of gasoline to leak January 12. Magellan officials reported that the spilled gasoline is being controlled in a containment area of the facility.
   Source: http://www.tulsaworld.com/news/gasoline-leaks-at-kansas-city-fuel-distribution-center/article_e8cba7a8-a961-54ca-9ff3-7fcb71d01d86.html

   For another story, see item **12**

[Return to top]

Chemical Industry Sector

4. *January 14, KMOV 4 St. Louis* – (Missouri) **Chemical fire injures worker near downtown St. Louis.** An acetone leak sparked a fire at a U.S. Paint chemical warehouse in St. Louis January 13, leaving one worker injured. The damage to the building was still under investigation after crews contained the blaze.
   Source: http://www.kmov.com/news/local/One-worker-injured-in-1st--alarm-chemical-fire-near-downtown-St-Louis-240029651.html

5. *January 13, U.S. Environmental Protection Agency* – (Maryland) **Warner Graham settles hazardous waste violations at Cockeysville, Md., facility.** Warner Graham, LLP agreed January 13 to pay $80,650 in a settlement with the U.S. Environmental Protection Agency to resolve claims that the company violated hazardous waste regulations at its Cockeysville, Maryland facility. The company also agreed to install a

less permeable floor beneath the product storage tank to minimize potential environmental risks.
Source: http://yosemite.epa.gov/opa/admpress.nsf/0/46067947d88a744685257c600044df7e?OpenDocument

6. *January 13, U.S. Department of Labor* – (Connecticut) **Connecticut manufacturer cited by US Labor Department's OSHA for chemical hazards; StanChem Inc., faces $55,300 in fines.** The U.S. Department of Labor's Occupational Safety and Health Administration cited StanChem Inc., for 13 safety hazards at its East Berlin, Connecticut manufacturing plant and proposed penalties totaling $55,300 after inspectors found several deficiencies in the plant's process safety management program.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=25380

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

7. *January 13, KSTP 5 St. Paul* – (Minnesota) **Prairie Island reactor gets new steam generators, returns to full power.** The Unit 2 reactor at the Prairie Island Nuclear Generating Plant in Red Wing returned to full power January 13 after being offline since September 2013 in order to replace two steam generators and perform a partial refueling.
Source: http://kstp.com/article/stories/S3280275.shtml?cat=12196

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

See item **1**

[Return to top]

Financial Services Sector

8. *January 13, KTLA 5 Los Angeles* – (California) **'Luger Bandit' sought in series of violent takeover bank robberies.** The FBI reported that a suspect known as the

"Luger Bandit" was linked to five violent bank robberies and one attempted robbery in Los Angeles, San Bernardino, and Riverside counties between June 2013 and January 8.
Source: http://ktla.com/2014/01/13/luger-bandit-sought-in-series-of-violent-takeover-bank-robberies/

9. *January 13, Softpedia* – (International) **22% of small US retailers are not PCI compliant, study shows.** Fortinet released the results of a survey conducted on 100 U.S. small and medium-sized businesses that found 22 percent are not Payment Card Industry Data Security Standard (PCI DSS) compliant, among other findings.
Source: http://news.softpedia.com/news/22-of-Small-US-Retailers-Are-Not-PCI-Compliant-Study-Shows-416424.shtml

10. *January 13, Washington Post* – (National) **Target says customers signing up for free credit monitoring after data breach.** Target announced January 13 that it is offering a year of free credit monitoring for customers following a breach of its systems that potentially exposed at least 100 million customers' personal or payment information.
Source: http://www.washingtonpost.com/business/technology/target-says-customers-signing-up-for-free-credit-monitoring-after-data-breach/2014/01/13/99fcce60-7c83-11e3-95c6-0a7aa80874bc_story.html

For another story, see item **27**

[Return to top]

Transportation Systems Sector

11. *January 14, NJ.com* – (New Jersey) **Route 17 southbound closed in Paramus for water main break.** New Jersey officials shut down Route 17 southbound at Ridgewood Avenue in Paramus for several hours January 14 because of a water main break.
Source:
http://www.nj.com/bergen/index.ssf/2014/01/route_17_southbound_closed_in_paramus_for_water_main_break.html

12. *January 13, Associated Press* – (North Dakota) **NTSB: 400,000 gallons of oil lost in ND derailment.** A preliminary National Transportation Safety Board (NTSB) report on a December 2013 collision between a derailed train and another train carrying oil in North Dakota found that 400,000 gallons of oil was lost in the incident, with about 25,000 gallons recovered. The NTSB is also investigating what role a broken axle may have played in the derailment of the first train.
Source : http://www.adn.com/2014/01/13/3271583/ntsb-400000-gallons-of-oil-lost.html

13. *January 13, KCNC 4 Denver* – (Colorado) **High winds close Highway 285.** High wind gusts near Fairplay, Colorado, forced officials to shut down Highway 285 for several

hours January 13.
Source: http://denver.cbslocal.com/2014/01/13/high-winds-closed-highway-285/

[Return to top]

Food and Agriculture Sector

14. *January 13, Associated Press* – (California) **California company Rancho Feeding Corporation recalls 40,000 pounds of meat.** Rancho Feeding Corporation of Petaluma recalled 41,683 pounds of meat products that were produced without a full federal inspection, leaving them unfit for human consumption, the U.S. Department of Agriculture's Food Safety and Inspection Service announced. The products were shipped to distribution centers and retail stores in California.
Source: http://www.nbcbayarea.com/news/local/California-Company-Rancho-Feeding-Corporation-Recalls-40000-Pounds-of-Meat-240010561.html

[Return to top]

Water and Wastewater Systems Sector

15. *January 14, Philadelphia Inquirer* – (Pennsylvania) **$3M damage estimate from water main break at shopping center.** A 48-inch water main that broke January 13 and flooded a shopping center in Philadelphia's East Falls area lost around 13 million gallons of water and caused at least $3 million in damage.
Source:
http://www.philly.com/philly/business/20140114__3M_damage_estimate_from_water-main_break_at_new_East_Falls_shopping_center.html

16. *January 14, WCHS 8 Charleston* – (West Virginia) **West Virginia American Water lifts ban in fifth area.** West Virginia American Water began lifting some water use bans January 13 in the Charleston area that were prompted by a chemical spill that leaked into the Elk River.
Source: http://www.wchstv.com/newsroom/eyewitness/140113_22349.shtml

17. *January 13, WCPO 9 Cincinnati* - (Ohio) **Greater Cincinnati Water Works prepared to deal with chemical spill in Ohio River, mayor says.** The Greater Cincinnati Water Works (GCWW) planned to shut down two water intake valves from the Ohio River January 14 to protect their water supply from chemicals that spilled into a tributary of the river in West Virginia. The threat was expected to pass within 24 hours.
Source: http://www.wcpo.com/news/local-news/hamilton-county/cincinnati/greater-cincinnati-water-works-prepared-to-deal-with-chemical-spill-in-ohio-river

18. *January 23, U.S. Department of Labor* - (Illinois) **Following complaint inspection, U.S. Department of Labor's OSHA proposes fines of 144,000 for U.S. Postal Service facility in Champaign, Ill.** A U.S. Postal Service facility in Champaign, Illinois, was cited by the Occupational Safety and Health Administration for eight

safety violations with proposed fines totaling $144,000.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=25383

For another story, see item **24**

[Return to top]

Healthcare and Public Health Sector

Nothing to report

[Return to top]

Government Facilities Sector

19. *January 14, USA Today; Associated Press* – (New Mexico) **2 teens critically injured in N.M. school shooting; 1 arrested.** Roswell police arrested a suspect January 14 following a shooting at Berrendo Middle School that left two people critically injured.
Source: http://www.usatoday.com/story/news/nation/2014/01/14/roswell-new-mexico-school-shooting-suspect/4472871/

20. *January 14, Associated Press* – (Texas) **Texas school district closed amid water dispute.** The La Villa Independent School District in Texas remained closed January 13 until further notice after the city shut off their water and sewer service amid a dispute over a bill and surcharge increases.
Source: http://news.msn.com/us/texas-school-district-closed-amid-water-dispute

21. *January 14, WRC 4 Washington, D.C.* – (Virginia) **Fairfax County school employee accused of refurbishing, selling stolen laptops.** Police arrested a Fairfax County Public Schools employee January 13 and charged him with two counts of embezzlement after they found 1,200 computers and 156 hard drives belonging to the school district, in his home. The employee is accused of taking used laptops, refurbishing them, and selling them online.
Source: http://www.nbcwashington.com/news/local/Craig-Soderberg-Fairfax-County-School-Employee-Charged-with-Embezzlement--239990251.html

22. *January 14, KHOU 11 Houston* – (Texas) **Bomb threat causes early-morning evacuation at Texas State University.** Texas State University's College Inn Hall was evacuated for more than 4 hours January 14 after a bomb threat. Nearby roads remained closed after students returned to their dorms.
Source: http://www.khou.com/news/texas-news/Bomb-threat-reported-on-the-campus-of-Texas-State-University-240068071.html

23. *January 14, Associated Press* – (Michigan) **Power outages cancel some Ferris State classes.** Ferris State University in Big Rapids was forced to cancel morning classes at

several buildings on campus January 14 due to two unrelated power outages January 13.
Source: http://www.detroitnews.com/article/20140114/SCHOOLS/301140058/1361/Power-outages-cancel-some-Ferris-State-classes

24. *January 13, Lexington Herald-Leader* – (Kentucky) **Schools out, thousands in Perry County remain without water after cold weather.** Authorities closed all schools in Perry County, Kentucky, January 14 due to the shutdown of production at a Hazard water plant when the intake iced over January 7 and left the schools without water. Nearly 2,000 water customers also remained without water January 13.
Source: http://www.kentucky.com/2014/01/13/3032601/thousands-in-perry-county-remain.html

For another story, see item **29**

[Return to top]

Emergency Services Sector

25. *January 13, KCPQ 13 Tacoma* – (Washington) **NORCOM investigating data breach of emergency calls.** The North East King County Regional Public Safety Communication Agency is investigating after its server was compromised and the medical response records of an estimated 6,000 individuals across 3 counties were potentially accessed, including 231 current and former firefighters. The agency was notified of the breach in December 2013 and the server is no longer in service.
Source: http://q13fox.com/2014/01/13/norcom-investigating-data-breach-of-emergency-calls/

[Return to top]

Information Technology Sector

26. *January 14, The Register* – (International) **Vulnerability leaves Cisco small biz routers wide open to attack.** Cisco issued a security advisory January 10 warning that some of its routers and networking products contain a vulnerability that could allow attackers to gain root access via an undocumented test interface. Exploit code for the vulnerability is available, though Cisco reported that they did not observe any widespread attacks based on it.
Source: http://www.theregister.co.uk/2014/01/14/cisco_small_business_router_flaw/

27. *January 14, Softpedia* – (International) **Mt. Gox fixes vulnerability that might have been exploited to hijack accounts.** A security researcher identified and reported several vulnerabilities in Bitcoin exchange Mt. Gox that could be used to hijack user accounts. Mt. Gox closed the vulnerabilities January 14.
Source: http://news.softpedia.com/news/MtGox-Fixes-Vulnerability-That-Might-Have-

Been-Exploited-to-Hijack-Accounts-416655.shtml

28. *January 13, CNET News* – (International) **Syrian Electronic Army hacks into Xbox Twitter accounts too.** Attackers claiming affiliation with the Syrian Electronic Army hacktivist group took control of the Twitter and Instagram accounts of Microsoft's Xbox gaming console January 11 and posted defacement messages. Microsoft regained control of the accounts later the same day.
Source: http://news.cnet.com/8301-1009_3-57617174-83/syrian-electronic-army-hacks-into-xbox-twitter-accounts-too/

For another story, see item **1**

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

See item **1**

[Return to top]

Commercial Facilities Sector

29. *January 14, KMGH 7 Denver* – (Colorado) **Denver police: suspect shot while using hostage as shield in escape attempt.** A man who took three individuals hostage at a Denver 7-Eleven January 13 was shot by police after refusing commands to release one hostage as he emerged from the store using them as a human shield. Several roads were closed and schools were placed on lockdown during the incident.
Source: http://www.thedenverchannel.com/news/local-news/denver-police-responding-to-possible-hostage-situation

30. *January 14, NBC News* – (Florida) **Retired cop guns down man for texting at Florida movie: sheriff.** One person was fatally shot and another was wounded after an altercation erupted at the Grove 16 Theatre in Wesley Chapel January 13. The suspect, a retired police captain, was restrained by an off-duty sheriff's deputy until authorities arrived.
Source: http://usnews.nbcnews.com/_news/2014/01/13/22292711-retired-cop-guns-down-man-for-texting-at-florida-movie-sheriff?lite

31. *January 14, KTVK 3 Phoenix* – (Arizona) **Strip mall fire closes several Phoenix businesses.** Officials are investigating a fire that broke out at a Phoenix strip mall

January 14, forcing several businesses to close due to smoke and water damage.
Source: http://www.azfamily.com/news/Strip-mall-fire-closes-several-Phoenix-businesses-240083811.html

32. *January 13, Pasadena Citizen* – (Texas) **Blaze displaces dozens at Pasadena apartment complex.** A fire broke out at the Cinnamon Ridge Apartment complex in Pasadena, Texas, January 13, causing the roof to collapse and leaving more than 50 residents displaced. Officials are investigating the cause of the fire.
Source: http://www.yourhoustonnews.com/pasadena/news/blaze-displaces-dozens-at-pasadena-apartment-complex/article_f79c764a-96b4-5e03-8997-7cda78fcad5e.html

For another story, see item **15**

[Return to top]

Dams Sector

33. *January 13, WGTU 29 Traverse County* – (Michigan**) Boardman River dam project enters $13 million phase.** The State of Michigan is beginning the second stage of a multi-million dollar removal of the Sabin and Boardman dams, and the modification of Union Street dam for the purpose of adding 13 miles of river channel for fish passage.
Source: http://www.upnorthlive.com/news/story.aspx?id=993891

[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.