



## Daily Open Source Infrastructure Report 22 January 2016

### Top Stories

- Researchers from Symantec discovered attackers were targeting finance departments of small and medium-sized businesses in India, the United Kingdom, and the U.S. to download financial software as well as other sensitive files. – *SecurityWeek* (See item [3](#))
- Freezing rain and sleet caused at least 70 crashes over a 10-hour period in Chattanooga January 20, forcing the temporary shutdown of Roberts Mill Road, the W Road, Highway 111, and Shoal Creek Road. – *Chattanooga Times Free Press* (See item [9](#))
- The Arkansas State agency’s board of commissioners approved a \$61 million loan for Little Rock Wastewater January 20 to conduct sewer system improvements at 2 wastewater treatment plants. – *Arkansas Democrat Gazette* (See item [13](#))
- The U.S. Department of Defense (DoD) announced January 20 that driver’s licenses from Minnesota, New Mexico, and several other states will no longer be accepted as proof of identity at DoD installations nationwide. – *U.S. Department of Defense* (See item [18](#))

---

### 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 21, Ann Arbor News* – (Michigan) **35-mile petroleum pipeline approved for southeast Michigan.** The Michigan Public Services commission approved a plan for the 35-mile Detroit Metro Access Pipeline January 21, which will stretch from Freedom Township to storage facilities in Romulus, and carry up to 90,000 barrels of refined petroleum daily. Construction is scheduled to begin during the summer of 2016. Source: [http://www.mlive.com/news/ann-arbor/index.ssf/2016/01/35-mile\\_refined\\_petroleum\\_pipe.html](http://www.mlive.com/news/ann-arbor/index.ssf/2016/01/35-mile_refined_petroleum_pipe.html)

## Chemical Industry Sector

Nothing to report

## Nuclear Reactors, Materials, and Waste Sector

Nothing to report

## Critical Manufacturing Sector

2. *January 21, Associated Press* – (Pennsylvania) **2 hurt when AK Steel plant furnace explodes in Pennsylvania.** Two employees at the AK Steel plant in Butler Township, Pennsylvania were injured and sent to an area hospital following an electric arc furnace explosion that occurred at the plant January 20. The company is investigating the cause of the blast. Source: <http://www.wtrf.com/story/31021084/2-hurt-when-ak-steel-plant-furnace-explodes-in-pennsylvania>

## Defense Industrial Base Sector

Nothing to report

## Financial Services Sector

3. *January 20, SecurityWeek* – (International) **Cybercriminals target bank accounts of firms in UK, US, India.** Researchers from Symantec discovered attackers were targeting finance departments of small and medium-sized businesses in India, the United Kingdom, and the U.S. to download financial software and steal files, passwords, and money by using stolen accounts to distribute malicious emails embedded with one of two remote access Trojans (RATs), that if deployed gives attackers complete control over the infected device and enables attackers to log keystrokes, among other actions. Researchers believe the attackers are based in Europe or the U.S. Source: <http://www.securityweek.com/cybercriminals-target-bank-accounts-firms-uk-us-india>
4. *January 20, Phoenix Business Journal* – (Arizona) **Former Kingman finance director**

**arrested for \$1.1M fraud.** The former Kingman Budget Analyst and Interim Finance Director was arrested and charged January 20 for 23 felony counts including theft, forgery, and misuse of public monies after she allegedly stole more than \$1 million from the city by using a city credit card for personal expenses, falsifying invoices to account for the charges, misappropriating funds from a bank account used to fund the city's Employees Benefits Trust, and altering account settings that granted her sole authority to initiate and approve transactions.

Source: <http://www.bizjournals.com/phoenix/news/2016/01/20/former-kingman-finance-director-arrested-for-1-1m.html>

## **Transportation Systems Sector**

5. *January 21, Fairfield-Suisun City Daily Republic* – (California) **Train tank cars with sulfuric acid derail in Martinez.** Crews spent 12 hours clearing the scene after 3 Union Pacific tank cars carrying sulfuric acid derailed January 20 near the Interstate 680 overpass in Martinez, California. No leaks or air quality issues were detected and authorities continue to investigate the incident.  
Source: <http://www.dailyrepublic.com/news/fairfield/train-tank-cars-with-sulfuric-acid-derail-in-martinez/>
6. *January 21, Cincinnati Enquirer* – (Connecticut) **Flight to CVG makes emergency landing in Connecticut.** A Delta Air Lines flight en route to Cincinnati was forced to return to Bradley International Airport in Hartford for an emergency landing January 20 due to a mechanical issue. Passengers were safely removed from the flight and transferred to another plane.  
Source: <http://www.cincinnati.com/story/news/2016/01/21/flight-cvg-makes-emergency-landing-connecticut/79104414/>
7. *January 20, WPLG 10 Miami* – (Florida) **Woman killed, 2 injured in crashes on Julia Tuttle Causeway.** Westbound lanes of the Julia Tuttle Causeway in Miami Beach were closed for approximately 5 hours January 20 due to an accident involving 3 vehicles that left 1 person dead and 2 others injured.  
Source: <http://www.local10.com/traffic/woman-killed-2-injured-in-i-195-crash>
8. *January 20, San Francisco Bay City News* – (California) **Big-rig collides with stolen sedan and overturns, spilling gas on Hwy 101.** Three southbound lanes of Highway 101 in San Jose were shut down for at least 5 hours January 20 after a vehicle collided with a semi-truck forcing the semi-truck to jackknife and overturn onto its side across the roadway. One injury was reported and the driver of the vehicle fled the scene.  
Source: <http://abc7news.com/traffic/big-rig-collides-with-stolen-sedan-and-overturns-spilling-gas-on-hwy-101/1167411/>
9. *January 20, Chattanooga Times Free Press* – (Tennessee) **Icy roads lead to 70 crashes in Chattanooga region, temps expected to warm today.** Freezing rain and sleet caused at least 70 crashes over a 10-hour period in Chattanooga January 20, forcing the temporary shutdown of Roberts Mill Road, the W Road, Highway 111, and Shoal Creek Road. North and southbound lanes of Interstate 75 were also shut down for

approximately 2 hours after steel from a semi-truck fell onto the roadway.

Source: <http://www.timesfreepress.com/news/local/story/2016/jan/20/i75-shut-down-near-ooltewah-traffic-woes-across-area/345650/>

10. *January 20, WITI 6 Milwaukee* – (Illinois) **Two dead in wrong-way, head-on collision that shut down I-43 SB near Oostburg.** Southbound lanes of Interstate 43 near Oostburg in Sheboygan were shut down for several hours January 20 while crews cleared the scene of an accident that left 2 people dead after 2 vehicles collided head-on due to a wrong-way driver.

Source: <http://fox6now.com/2016/01/20/crash-closes-i-43-sb-near-oostburg-in-sheboygan-county/>

For another story, see items [1](#)

## **Food and Agriculture Sector**

11. *January 21, U.S. Department of Agriculture* – (Tennessee) **Snapp's Ferry Packing Company recalls beef product due to possible E. coli O157:H7 contamination.** Alton, Tennessee-based Snapp's Ferry Packaging Company issued a recall January 20 for approximately 410 pounds of its Ground Beef products packaged in 5-pound bags after an investigation from an ongoing illness revealed positive traces of E. coli O157:H7 in the products. The product was distributed only to restaurants in the Knoxville, Tennessee area.

Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-007-2016-release>

12. *January 20, KPIX 5 San Francisco* – (California) **Benicia Popcorn Factory shut down for weeks over mice infestation.** Officials from Kettlepop LLC reported January 20 that its popcorn factory in Benicia was shut down for two weeks and will remain shut down while pest control crews eradicate a mouse infestation found alongside the popcorn's raw materials. Officials reported all goods produced at the plant were destroyed after finding the mice infestation.

Source: <http://sanfrancisco.cbslocal.com/2016/01/20/benicia-popcorn-factory-shut-down-for-weeks-over-mice-infestation/>

## **Water and Wastewater Systems Sector**

13. *January 21, Arkansas Democrat-Gazette* – (Arkansas) **Little Rock utility cleared for \$61M for work at 2 sewer plants.** The Arkansas State agency's board of commissioners approved a \$61 million loan for Little Rock Wastewater January 20 to conduct sewer system improvements at Adams Field and Fourche Creek wastewater treatment plants to help prevent overflows during heavy rains. The loan is part of an estimated \$220 million request from the utility for improvement projects around the State.

Source: <http://www.arkansasonline.com/news/2016/jan/21/lr-utility-cleared-for-61m-for-work-at-/?f=news-arkansas>

14. *January 20, KCNC 4 Denver* – (Colorado) **9 water main breaks repaired, water restored to 20,000 people.** Crews repaired 9 water main breaks that affected 20,000 residential and business customers in Denver and forced the closure of 4 area schools January 20. The cause of the breaks remains under investigation.  
Source: <http://denver.cbslocal.com/2016/01/20/water-main-breaks-force-closure-of-4-schools/>

## **Healthcare and Public Health Sector**

Nothing to report

## **Government Facilities Sector**

15. *January 21, WEWS 5 Cleveland* – (Ohio) **Saint Ignatius High School closed due to bomb threat.** Classes at Saint Ignatius High School in Cleveland were cancelled January 21 due to a phoned bomb threat. A bomb squad was dispatched to the site to search for anything suspicious.  
Source: <http://www.newsnet5.com/news/local-news/cleveland-metro/saint-ignatius-high-school-closed-due-to-bomb-threat>
16. *January 21, Lake County News-Sun* – (Illinois) **Truck driver charged after crash injures 9 children on school bus in Beach Park.** A chain-reaction crash January 20 in Beach Park involving a school bus and 2 semi-trucks left 9 Kenneth Murphy Elementary School students injured when a semi-truck failed to stop and crashed into the school bus, causing it to move forward and crash into another semi-truck.  
Source: <http://www.chicagotribune.com/suburbs/lake-county-news-sun/news/ct-lns-bus-crash-beach-park-st-0121-20160120-story.html>
17. *January 21, Boston Globe* – (Massachusetts) **Milford High School closed after getting bomb threat.** An emailed bomb threat targeting Milford High School in Boston forced the school's closure January 21 while officials searched the campus. Police cleared the scene and deemed it safe once nothing suspicious was found.  
Source: <https://www.bostonglobe.com/metro/2016/01/21/milford-high-school-closed-after-getting-threat/knDtdczVfks65PFicLjTrM/story.html>
18. *January 20, U.S. Department of Defense* – (National) **Licenses from 5 states banned at DoD bases.** The U.S. Department of Defense (DoD) announced January 20 that driver's licenses from Minnesota, New Mexico, Illinois, Missouri, and Washington will no longer be accepted as proof of identity at DoD installations nationwide as a result of the REAL ID Act of 2005.  
Source: <http://www.defense.gov/News-Article-View/Article/643615/licenses-from-5-states-banned-at-dod-bases>
19. *January 20, WFMZ 69 Allentown* – (Pennsylvania) **Bomb threat forces evacuation of Northampton County Courthouse in Easton.** The Northampton County Courthouse in Easton was evacuated for 3 hours January 20 and all proceedings for the day were cancelled due to a bomb threat. Authorities issued an all clear after conducting a search

of the building.

Source: <http://www.wfmz.com/news/news-regional-lehighvalley/sheriffs-office-bomb-threat-forces-evacuation-of-northampton-county-courthouse/37533170>

20. *January 20, Bangor Daily News* – (Maine) **Bomb threat closes Machias high school.** Classes at Machias Memorial High School in Maine were scheduled to resume January 21 following the school's closure January 20 due to a hoax bomb threat which was communicated to a staff member. Officials are investigating the incident.  
Source: <http://bangordailynews.com/2016/01/20/news/down-east/police-mum-on-closing-of-machias-high-school/?ref=topStories7>

For another story, see item [14](#)

## Emergency Services Sector

See item [27](#)

## Information Technology Sector

21. *January 21, Softpedia* – (International) **Threat group uses dating sites to build a botnet of vulnerable home routers.** Damballa security researchers reported that a Linux ELF binary, a variant of TheMoon worm, was targeting Home Network Administration Protocol (HNAP) by using adult dating Web sites to infect home routers and prevents consumers from using their routers' inbound ports via a malicious iframe embedded on the malicious web pages. Researchers reported the worm is spread by opening outbound ports on the router to infect other routers.  
Source: <http://news.softpedia.com/news/threat-group-uses-dating-sites-to-build-a-botnet-of-vulnerable-home-routers-499209.shtml>
22. *January 21, SecurityWeek* – (International) **Google Chrome 48 patches 37 security flaws.** Google released its newest web browser version, Chrome 48 for Microsoft Windows, Apple Mac, and Linux users that patches 37 security vulnerabilities including a bad cast flaw in V8, a use-after-free bug in PDFium, and six other vulnerabilities found by external researchers, among other patched flaws. In addition, company officials reported the updated version included a series of improvements to the browser.  
Source: <http://www.securityweek.com/google-chrome-48-patches-37-security-flaws>
23. *January 21, Help Net Security* – (International) **Fake Facebook emails deliver malware masquerading as audio message.** Researchers from Comodo reported that a similar malware, previously targeting WhatsApp users, has been targeting Facebook users to steal information about a victim's computer and send the stolen information to a command-and-control (C&C) server where attackers can send additional malware via malicious emails embedded with a variant of the Nivdort information-stealing Trojan. Once the malicious email is open, the malware will replicate itself into "C:/" directory and add a Windows Registry entry, allowing the malware to run automatically after each restart or shutdown of the device.

Source: [http://www.net-security.org/malware\\_news.php?id=3191](http://www.net-security.org/malware_news.php?id=3191)

24. *January 20, Softpedia* – (International) **Malvertising returns on Microsoft’s MSN portal.** Security researchers from Malwarebytes reported that Microsoft’s MSN portal was susceptible to malvertising campaigns via the Nuetrino and RIG exploit kits (EK) by creating new domains used a few days prior to each attack or hiding behind the CloudFlare service. Researchers advised users to use a security product to block incoming malware.

Source: <http://news.softpedia.com/news/malvertising-returns-on-microsoft-s-msn-portal-499179.shtml>

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto: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. *January 21, KTVI 2 St. Louis* – (Missouri) **Fire rips through DeSoto bowling alley.** A commercial building housing the White Mule Saloon and the Ball Creek Bowling Alley in Desoto, Missouri was heavily damaged January 20 after a three-alarm fire caused the roof of the building to collapse and prompted three fire counties to respond to the incident. No injuries were reported and the State Fire Marshal’s office is investigating.

Source: <http://fox2now.com/2016/01/21/fire-rips-through-desoto-bowling-alley/>

26. *January 21, Bay News 9 Tampa Bay* – (Florida) **Fire tears through Tampa apartment building overnight.** A 2-alarm fire at the Westchester Manor Apartments in Tampa sustained extensive damage January 21 after the fire began in 1 apartment unit and spread to surrounding units, displacing 14 residents. The State Fire Marshal’s office is investigating the incident and no injuries were reported.

Source:

[http://www.baynews9.com/content/news/baynews9/news/article.html/content/news/articles/bn9/2016/1/21/fire\\_tears\\_through\\_t.html](http://www.baynews9.com/content/news/baynews9/news/article.html/content/news/articles/bn9/2016/1/21/fire_tears_through_t.html)

27. *January 20, KXAS 5 Fort Worth* – (Texas) **Fire truck slams into Dairy Queen in Collin County.** A Dairy Queen restaurant in Farmersville, Texas, sustained extensive damage and was closed indefinitely January 20 after a Greenville Fire-Rescue fire truck, being transferred to its fire station, crashed into the restaurant and caused part of the front wall to collapse. Two people sustained non-life threatening injuries and the incident is under investigation.

Source: <http://www.nbcdfw.com/news/local/Fire-Truck-Slams-Into-Dairy-Queen-in->

[Collin-County-365943971.html](#)

For another story, see item [14](#)

## **Dams Sector**

28. *January 20, KOVR 13 Stockton* – (California) **Cofferdam breach halted at Folsom Dam as crews ready for next storm.** Crews stabilized a temporary cofferdam built to hold back water at the Folsom Lake spillway construction site in California January 20 after a leak was spotted forcing workers to evacuate and all construction work to be stopped. Officials are still assessing whether to pump out the water or flood the area. Source: <http://sacramento.cbslocal.com/2016/01/20/cofferdam-breach-halted-at-folsom-dam-as-crews-ready-for-next-storm/>



**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 <a href="mailto:cikr.productfeedback@hq.dhs.gov">cikr.productfeedback@hq.dhs.gov</a> or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the <a href="#">DHS Daily Open Source Infrastructure Report</a> and follow instructions to <a href="#">Get e-mail updates when this information changes</a> .
Removal from Distribution List:	Send mail to <a href="mailto:support@govdelivery.com">support@govdelivery.com</a> .

---

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@hq.dhs.gov](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://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.