Homeland Security

Daily Open Source Infrastructure Report
05 March 2014

Top Stories

- Officials are investigating after two miners were injured and then rescued after the roof of the D and F Mine in Schuylkill County, Pennsylvania, partially collapsed and trapped them March 3. – *WNEP 16 Scranton* (See item **1**)

- Burlington Northern Santa Fe (BNSF) officials began bussing passengers around an avalanche that blocked BNSF railway tracks south of Glacier National Park in Montana March 2. – *Montana Standard* (See item **8**)

- Classes were cancelled and Trinity High School in Dickinson, North Dakota, was shut down indefinitely after a March 3 fire caused extensive damage to the building. – *KXMC 13 Minot* (See item **17**)

- Security researchers found that around 300,000 small office/home office routers have been compromised and had their DNS settings changed in order to allow them to perform man-in-the-middle attacks. – *Help Net Security* (See item **21**)

Fast Jump Menu

PRODUCTION INDUSTRIES	SERVICE INDUSTRIES
• Energy	• Financial Services
• Chemical	• Transportation Systems
• Nuclear Reactors, Materials, and Waste	• Information Technology
• Critical Manufacturing	• Communications
• Defense Industrial Base	• Commercial Facilities
• Dams	**FEDERAL and STATE**
SUSTENANCE and HEALTH	• Government Facilities
• Food and Agriculture	• Emergency Services
• Water and Wastewater Systems	
• Healthcare and Public Health	

Energy Sector

1. *March 3, WNEP 16 Scranton* – (Pennsylvania) **Coal miners rescued in Schuylkill County.** Officials are investigating after two miners were injured when the roof of the D and F Mine in Schuylkill County partially collapsed and trapped them March 3. The injured miners were rescued and transported on a medical helicopter.
Source: http://wnep.com/2014/03/03/coal-miners-trapped-in-schuylkill-county/

[Return to top]

Chemical Industry Sector

See item **7**

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

2. *March 3, Kalamazoo Gazette* – (Michigan) **Piece of metal lodged in reactor at Palisades Nuclear Power Plant.** Operators at the Palisades Nuclear Power Plant in Covert Township discovered a piece of metal from a broken impeller blade lodged in the plant's reactor vessel during a scheduled refueling and maintenance outage. Efforts to remove the metal debris were unsuccessful but plant operators do not believe the debris poses a threat to operations or safety.
Source: http://www.mlive.com/news/kalamazoo/index.ssf/2014/03/piece_of_metal_reactor_lodged.html

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

3. *March 4, U.S. Securities and Exchange Commission* – (Illinois) **Federal grand jury indicts CEO of Chicago-area company accused of defrauding investors in multi-**

million dollar stock scam. A federal grand jury returned an indictment February 28 against the CEO and president of InfrAegis Inc., on charges of allegedly using false information to obtain more than $9 million from investors between 2007 and 2013.
Source: http://www.sec.gov/litigation/litreleases/2014/lr22935.htm

4. *March 4, Softpedia* – (International) **Bitcoin bank Flexcoin shuts down after hackers emptied hot wallet.** Bitcoin bank Flexcoin announced March 4 that it was shutting down operations after attackers leveraged a vulnerability and withdrew all Bitcoins from the bank's 'hot' wallet, around 900 Bitcoins worth over $600,000. Customers' Bitcoins stored in offline 'cold' wallets were unaffected.
Source: http://news.softpedia.com/news/Bitcoin-Bank-Flexcoin-Shuts-Down-After-Hackers-Emptied-Hot-Wallet-430469.shtml

5. *March 3, Centre Daily Times* – (Pennsylvania) **Police: I-80 car search nets 116 fake credit cards hidden in cereal box.** A New Jersey woman was arrested March 1 in Marion Township, Pennsylvania, after a traffic stop on Interstate 80 led police to discover 115 fraudulent credit cards sealed in a cereal box.
Source: http://www.centredaily.com/2014/03/03/4065507/police-i-80-car-search-nets-116.html

[Return to top]

Transportation Systems Sector

6. *March 4, WSBT 22 South Bend* – (Michigan) **Police: Speed, reckless driving cause deadly car-semi crash on I-94.** A portion of the eastbound lanes on Interstate 94 between Benton Harbor and Coloma were closed for over 3 hours March 3 after a car weaving in and out of traffic rear-ended a semi-truck, killing the driver of the car.
Source: http://www.wsbt.com/news/local/crash-closes-part-of-i94-in-berrien-county/24782656

7. *March 4, KSLA 12 Shreveport* – (Louisiana) **I-49 in Natchitoches back open after hazmat spill & fire.** HAZMAT crews worked March 4 to clear the site of an overturned semi-truck that was carrying several thousand gallons of flammable, hazardous materials near Natchitoches. The accident prompted closure of a portion of Interstate 49 for more than 2 hours.
Source: http://www.ksla.com/story/24877158/part-of-i-49-closed-after-tanker-with-flammable-material-overturns

8. *March 4, Montana Standard* – (Montana) **Avalanche blocks BNSF line near Glacier Park.** Burlington Northern Santa Fe (BNSF) officials began bussing passengers around an avalanche that blocked BNSF railway tracks south of Glacier National Park March
Source: http://mtstandard.com/news/state-and-regional/avalanche-blocks-bnsf-line-near-glacier-park/article_a075c37c-a37b-11e3-b201-0019bb2963f4.html

9. *March 4, Associated Press* – (California) **Woman dies, husband survives small plane**

crash. The Federal Aviation Administration (FAA) is investigating a single-engine airplane crash that killed a woman and critically injured her husband March 3 about 6 miles from California's Truckee Tahoe Airport.
Source : http://lasvegassun.com/news/2014/mar/03/single-engine-plane-crashes-near-truckee-airport/

10. *March 3, Lower Columbia Daily News* – (Washington) **Pedestrian killed on Interstate 5 near Woodland.** A section of Interstate 5 in Woodland was closed for nearly 5 hours after a semi-truck struck and killed a man standing in the middle of the road March 3.
Source : http://tdn.com/news/local/pedestrian-killed-on-interstate-near-woodland/article_f53b2f46-a2ef-11e3-9cfa-001a4bcf887a.html

For another story, see item **31**

Food and Agriculture Sector

11. *March 1, KOKI 23 Tulsa* – (Oklahoma) **Restaurant under investigation after 40 people became ill in Wagoner County.** The Wagoner County Health Department is investigating after as many as 40 people reportedly contracted viral gastroenteritis from eating at Las Fuentes restaurant in Oklahoma February 23.
Source: http://www.fox23.com/news/local/story/Restaurant-under-investigation-after-40-people/9jZLXT7t5kScJQnYFJiWLg.cspx

Water and Wastewater Systems Sector

12. *March 3, KGO 7 San Francisco* – (California) **Water main break in Concord leaves big hole in San Miguel Road.** A 36-inch water pipe burst underneath San Miguel Road in Concord, California, March 3, causing authorities to shut down the road for several hours and a large geyser to spray water into the air. An estimated 10 to 12 hours was needed to fix the problem and clean up the mess caused by the water main break.
Source: http://abclocal.go.com/kgo/story?section=news/local/east_bay&id=9453306

13. *March 3, Cache Valley Daily* – (Utah) **Water boiling order for Trenton residents.** Residents of Trenton, Utah, were placed under a mandatory boil water order that could last a few months after murky colored water was found in the city's drinking system, leading officials to think E. coli, cryptosporidium, giardia, and other bacteria could be contaminating the water.
Source: http://www.cachevalleydaily.com/news/local/article_c6188dec-a34b-11e3-82b7-0017a43b2370.html

Healthcare and Public Health Sector

14. *March 4, SC Magazine* – (National) **Stolen laptop leads to compromised unencrypted personal data.** AppleCare Insurance Services notified individuals who have enrolled in or discussed health care plan options with one agent that their personal information may have been compromised after the agent's unencrypted laptop was stolen.
Source: http://www.scmagazine.com//stolen-laptop-leads-to-compromised-unencrypted-personal-data/article/336571/

15. *March 3, Providence Journal* – (Rhode Island) **Health department says some in RI might have been exposed to measles.** The Rhode Island Department of Health released a statement March 2 announcing that it is working with two area hospitals to determine if any patients were exposed to an individual who likely had measles after the individual was in both hospitals the week of February 24.
Source: http://www.providencejournal.com/breaking-news/content/20140303-health-department-says-some-in-ri-might-have-been-exposed-to-measles.ece

16. *March 1, Sherman/Denison Herald Democrat* – (Texas) **Security breached, patient information compromised at doctor's office.** A Sherman, Texas doctor's office was broken into January 5 and thieves took computers and at least one hard drive which contained patients' personal information. The practice notified patients of the security breach and is currently upgrading their security system while continuing to investigate the incident.
Source: http://heralddemocrat.com/news/local/security-breached-patient-information-compromised-office-dr-jm-benson

Government Facilities Sector

17. *March 4, KXMC 13 Minot* – (North Dakota) **Dickinson Trinity High School up in flames.** Classes were cancelled and Trinity High School in Dickinson was shut down indefinitely after a March 3 fire caused extensive damage to the building. Authorities are investigating the cause of the fire while classes resume at nearby schools.
Source: http://www.kxnet.com/story/24874871/trinity-high-school

For another story, see item **18**

Emergency Services Sector

18. *March 3, Winston-Salem Journal* – (North Carolina) **County employees sent to hospital after chemical spill at jail.** A toxic dry cleaning chemical spilled when a worker removed an unused dry cleaning machine at the county jail in Forsyth County March 3, prompting almost 20 employees to be transported to an area hospital for

evaluation. Crews contained the spilled perchloroethylene and cleaned the area.
Source: http://www.journalnow.com/news/local/county-employees-sent-to-hospital-after-chemical-spill-at-jail/article_7809cffa-a308-11e3-884e-001a4bcf6878.html

19. *March 3, WSFA 12 Montgomery* – (Alabama) **Inmates hospitalized after Elmore prison brawl.** Corrections officers stopped a fight between inmates at the Elmore Correctional Facility in Alabama March 2 that left eight inmates injured. The incident is under investigation.
Source: http://www.wsfa.com/story/24872858/inmates-hospitalized-after-elmore-prison-brawl

Information Technology Sector

20. *March 4, Dark Reading* – (International) **Researchers create legal botnet abusing free cloud service offers.** Researchers presenting at the RSA Conference the week of February 24 demonstrated how they were able to create a botnet by abusing trial accounts for several platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) offers. The botnet was created by automating PaaS and IaaS trial sign-up processes and could be used to perform massive port scans, Bitcoin mining, and to manipulate sweepstakes, among other tasks.
Source: http://www.darkreading.com/researchers-create-legal-botnet-abusing/240166428

21. *March 4, Help Net Security* – (International) **300,000 routers compromised in DNS hijacking campaign.** Researchers with Team Cymru found that around 300,000 small office/home office routers have been compromised and had their DNS settings changed to two IP addresses in the U.K. in order to allow them to perform man-in-the-middle (MitM) attacks. The researchers found that the attack dates to at least mid-December 2013 and has mostly affected routers in Europe and Asia.
Source: http://www.net-security.org/secworld.php?id=16473

22. *March 4, Softpedia* – (International) **19 security fixes included in latest Chrome 33 update.** Google released an update for its Chrome browser, Chrome version 33.0.1750, which addresses 19 security issues.
Source: http://news.softpedia.com/news/19-Security-Fixes-Included-in-Chrome-33-0-1750-146-Update-430494.shtml

23. *March 3, Softpedia* – (International) **Flaw in Yahoo! Suggestions allowed hackers to delete 1.5 million posts and comments.** A security researcher identified and reported an Insecure Direct Object Reference Vulnerability (IDORV) in Yahoo's Suggestions Web site that could have allowed attackers to escalate their privileges and delete large amounts of posts and comments. Yahoo addressed the issue within 2 days.
Source: http://news.softpedia.com/news/Flaw-in-Yahoo-Suggestions-Allowed-Hackers-to-Delete-1-5-Million-Posts-and-Comments-430303.shtml

24. *March 3, Threatpost* – (International) **Four vulnerabilities found in Oracle Demantra.** Researchers at Portcullis identified four vulnerabilities in Oracle's Demantra business software that could allow attackers to steal sensitive information, carry out phishing attacks, modify application content, or perform other attacks. Source: http://threatpost.com/four-vulnerabilities-found-in-oracle-demantra/104574

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

Nothing to report

[Return to top]

Commercial Facilities Sector

25. *March 4, WNYF 28 Watertown* – (New York) **Watertown apartment building evacuated.** Residents of the Brighton Apartments building in Watertown were evacuated for several hours March 4 due to carbon monoxide contamination caused by a boiler malfunction at an adjacent building that is under renovation. Source: http://www.wwnytv.com/news/local/CO-Contamination-Forces-Apartment-Building-Evacuation-248348861.html

26. *March 3, Royal Oak Daily Tribune* – (Michigan) **County HAZMAT, State DEQ workers investigating massive fuel spill at Auburn Hills business.** Crews responded March 3 to an RGIS office building in Auburn Hills after approximately 4,000 gallons of diesel fuel spilled from the business' backup generator and entered a nearby private storm drain that feeds into a retention pond on the property. An environmental clean-up company was hired to handle the spill and investigations are underway to determine if the fuel leaked into the public sanitary system. Source: http://www.dailytribune.com/general-news/20140303/county-hazmat-state-deq-workers-investigating-massive-fuel-spill-at-auburn-hills-business

27. *March 3, KFSN 30 Fresno* – (California) **Water leak damages lobby of Holiday Inn in downtown Fresno.** Crews shut off power to the Holiday Inn in downtown Fresno for nearly 3 hours March 3 after a 3-inch water line ruptured and gushed about 3,000 gallons of water into the hotel's lobby. Source: http://abclocal.go.com/kfsn/story?section=news/local&id=9453144

28. *March 3, KVVU 5 Las Vegas* – (Nevada) **26 injured when truck plows through Las**

Vegas store. Nine people were hospitalized and 17 others were injured after the driver of a pickup truck lost control and crashed through the front of a Food 4 Less grocery store in Las Vegas March 1. The store reopened March 2.
Source: http://www.fox5vegas.com/story/24861291/elderly-woman-drives-car-into-grocery-store

29. *March 3, Tampa Tribune* – (Florida) **Brandon Dillard's reopens after evacuation during search for suspects.** Dillard's department store at the Westfield Brandon mall near Tampa was evacuated and closed for over 2 hours March 3 while authorities searched for 3 burglary suspects that led police on a high speed chase before crashing their car and running into the store.
Source: http://tbo.com/brandon/dillards-in-brandon-evacuated-during-search-for-suspects-20140303/

30. *March 3, Associated Press; Sioux City Journal* – (Iowa) **Firefighter injured while battling Sioux City fire.** Two firefighters were injured and more than two dozen residents were displaced after a fire broke out and damaged at least 12 units at the Glen Oaks Apartments in Sioux City March 3.
Source: http://siouxcityjournal.com/ap/state/firefighter-injured-while-battling-sioux-city-fire/article_8033d69c-a6af-5e57-95a1-ee3a629543d2.html

[Return to top]

Dams Sector

31. *March 4, Associated Press* – (Wisconsin) **Thick ice stalls lock, dam reopening.** The reopening of Lock and Dam 8 near Genoa, Wisconsin, was pushed back by a week to March 17 as thick ice on the upper Mississippi River prevents navigation. Workers will use the additional time to fully complete the renovation and maintenance that was started December 2.
Source: http://www.leadertelegram.com/news/daily_updates/article_89faa32c-a3a0-11e3-a05e-001a4bcf887a.html

[Return to top]

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.