Daily Open Source Infrastructure Report
25 January 2016

Top Stories

- An impending snowstorm along the east coast prompted more than 4,500 flight cancellations nationwide, school closures across several States, and the shutdown of public transportation in Washington, D.C. January 22 and January 23. – *CNN* (See item **5**)
- A blizzard warning prompted the closure of nearly all Washington, D.C., Maryland, and Virginia schools January 22 after officials declared states of emergency January 21. – *WRC 4 Washington, D.C.* (See item **9**)
- The Georgia Department of Corrections charged 4 current officers, 11 former officers, 18 inmates, and 21 civilians in connection to a corruption, fraud, and money laundering scheme at the Autry State Prison in Pelham January 21. – *WMAZ 13 Macon* (See item **12**)
- AMX released a firmware update for its NX-1200 device, a central controller used by the White House, after an SEC Consult discovered backdoor accounts on older versions of the device. – *Softpedia* (See item **14**)

Fast Jump Menu

Energy Sector

1. *January 21, Associated Press* – (Alabama) **Alabama couple ordered to return $1.6 million in BP claim money.** The owners of Alabama-based Vision Design Management were ordered to repay more than $1.6 million in claim money following the 2010 BP Deepwater Horizon explosion in the Gulf of Mexico after a Federal court determined that the company submitted fraudulent revenue documents to the Deepwater Horizon Economic Claims Center, and were wrongfully awarded over $2.1 million.
   Source: http://www.al.com/news/index.ssf/2016/01/alabama_couple_ordered_to_retu.html

2. *January 21, Colorado Springs Gazette* – (Colorado) **Colorado Springs Utilities board seals fate for Drake unit.** The Colorado Springs Utilities board announced January 20 that Unit 5 at the coal-fired Martin Drake Power Plant will close by the end of 2017 in order to avoid the high economic cost of continued operations and maintenance of the unit.
   Source: http://gazette.com/colorado-springs-utilities-board-decides-future-of-drake-unit/article/1568245

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. *January 21, KTLA 5 Los Angeles* – (California) **Hourslong search for 2 bank robbery suspects ends in Culver City; 2 others detained.** Two schools were placed on lockdown and a T.J. Maxx store was evacuated January 21 after four armed men reportedly fired shots at a One West Bank in Culver City and robbed the bank of an undisclosed amount of funds. Two of the four suspects were detained outside of the bank and the retail store, and no injuries were reported.
   Source: http://ktla.com/2016/01/21/schools-on-lockdown-t-j-maxx-evacuated-amid-search-for-bank-robbers-in-culver-city/

4. *January 21, Sacramento Bee* – (California) **Sacramento woman pleads guilty to role in credit card fraud conspiracy.** The U.S. Attorney's Office announced that a Sacramento woman pleaded guilty January 21 to conspiracy to commit access-device fraud and aggravated identity theft charges after she was linked to a credit card scheme involving four others who allegedly committed mail fraud, obtained at least 500 counterfeit credit and debit cards, and made over $186,000 in fraudulent purchases at retail stores in the Sacramento area from July 2014 – April 2015.
Source: http://www.sacbee.com/news/local/crime/article55915090.html

For another story, see item **1**

Transportation Systems Sector

5. *January 22, CNN* – (National) **Snowstorm threaten east coast; D.C., Baltimore under blizzard warnings.** An impending snowstorm along the east coast prompted more than 4,500 flight cancellations nationwide, school closures across several States, the shutdown of the Washington Metropolitan Area Transit Authority (Metro) in Washington, D.C., and state of emergency issuances along the Atlantic coast for January 22 and January 23. Preparations for the storm follow snowfall January 20 in Maryland and Virginia, which caused 767 accidents and responses to 392 calls for disabled vehicles, among other incidences.
Source: http://www.cnn.com/2016/01/21/us/winter-snowstorm-washington-blizzard/

6. *January 22, KTVI 2 St. Louis –* (Missouri) **Pedestrian struck, killed on WB I-64 before Hampton.** Westbound lanes of Interstate 64/40 in St. Louis were shut down for nearly 4 hours January 22 after a pedestrian was hit and killed while walking on the highway.
Source: http://fox2now.com/2016/01/22/accident-closes-two-left-lanes-on-wb-i-64-before-hampton-2/

7. *January 21, Chicago Sun-Times* – (Illinois) **Freight train derailment causing delays on Metra Rock Island line.** A partly owned Iowa Interstate Railroad freight train derailed January 21 in south Blue Island in Illinois causing delays for outbound trains on Metra's Rock Island Line for several hours while crews worked to remove the derailed cars. Metra notified customers of its modified train schedule.
Source: http://chicago.suntimes.com/news/7/71/1269014/hold-freight-train-derailment-causes-delays-rock-island-line

Food and Agriculture Sector

8. *January 21, U.S. Food and Drug Administration* – (National) **Mahina Mele Farms, LLC recalls macadamia nut products due to possible health risk.** Mahina Mele Farms, LLC issued a recall for seven varieties of its macadamia nuts products January 21 after routine testing revealed the presence of Salmonella in the macadamia nuts. The affected products were distributed in retail stores nationwide and no illnesses have been reported.

Source: http://www.fda.gov/Safety/Recalls/ucm482670.htm

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

9. *January 22, WRC 4 Washington, D.C.* – (Washington, D.C.; Maryland; Virginia) **Blizzard may dump 30 inches of snow on DC area; first flakes begin at noon.** A blizzard warning prompted the closure of nearly all Washington, D.C., Maryland, and Virginia schools January 22 after officials declared states of emergency January 21. Federal government and local government offices were also closed or issued early closures as a precaution.
Source: http://www.nbcwashington.com/news/local/Icy-Roads-Close-Delay-Schools-Ahead-of-Expected-Blizzard-366030031.html

10. *January 21, KHSL 12 Chico* – (California) **Chlorine leak closes Anderson River Park.** Anderson River Park in California was closed indefinitely January 21 following a reported chlorine leak from a cylinder at a treatment plant which led to an evacuation of the area. One worker was treated on site and the leak was isolated and contained.
Source: http://www.actionnewsnow.com/news/chlorine-leak-closes-anderson-river-park/

11. *January 21, Racine County Journal Times* – (Wisconsin) **School buses crash on the way to Camp MacLean, 10 report injuries.** Ten students from Barrington High School in Illinois, who were en route to YMCA Camp MacLean in Wisconsin, reported injuries following an accident between two buses in Fox Lake January 21.
Source: http://journaltimes.com/news/local/school-buses-crash-on-the-way-to-camp-maclean-report/article_50293ac5-8d91-5a93-834f-953eb027ee63.html

For additional stories, see items **3** and **5**

Emergency Services Sector

12. *January 21, WMAZ 13 Macon* – (Georgia) **54 indicted in Georgia state prison conspiracy case.** The Georgia Department of Corrections announced January 21 that 4 current officers, 11 former officers, 18 inmates, and 21 civilians were charged in connection to a corruption, fraud, and money laundering scheme at the Autry State Prison in Pelham in which the defendants allegedly used contraband cell phones to call and mislead victims into falsely thinking that they failed to report to jury duty and ordered them to pay bogus fines.
Source: http://www.13wmaz.com/story/news/local/georgia/2016/01/21/54-indicted-in-

georgia-state-prison-conspiracy-case/79131248/

Information Technology Sector

13. *January 22, ZDNet* – (International) **TeslaCrypt flaw opens the door to free file decryption.** A security researcher discovered that the TeslaCrypt ransomware and variants of TeslaCrypt 2.0 contained a design flaw in how the ransomware's encryption keys were stored in a victim's computer following the discovery that a new Advanced Encryption Standard (AES) key was generated during each encryption session, revealing that researchers could use specialized programs to retrieve prime numbers of the stored keys to reconstruct a decryption key. Researchers developed software that generates decryption keys for TeslaCrypt files with the extensions .ECC, .EZZ, .EXX, .XYZ, .ZZZ, .AAA, .ABC, .CCC, and .VVV.
Source: http://www.zdnet.com/article/teslacrypt-vulnerability-exposes-ransomed-files-to-free-cracking/

14. *January 21, Softpedia* – (International) **Backdoor account found on devices used by White House, US military.** AMX released a firmware update for its NX-1200 device, a central controller used by the White House for conference room equipment, after a security researcher from SEC Consult discovered that older versions of the devices' firmware were embedded with a series of backdoor accounts under the username, "BlackWidow" and "1MB@tMaN" that could have allowed attackers to spy on users and hack the device. A source code named "setUpSubtleUserAccount" was found to set up hidden user accounts without appearing in the devices' configuration screen, posing several vulnerabilities.
Source: http://news.softpedia.com/news/backdoor-found-in-devices-used-by-white-house-us-military-499239.shtml

15. *January 21, Softpedia* – (International) **Kovter malware victims were secret zombies in the ProxyGate proxy network.** Security researchers from Forcepoint detected that the malware, Kovter was recently distributed through an email campaign attached with ZIP files that when opened, executes a JavaScript file and connects to a web server without the users' consent and downloads the Kovter malware, and two additional payloads including the Miuref adware and the ProxyGate installer. Researchers believe the author of the campaign may be running other malicious campaigns through ProxyGate's network to increase his available proxy output Internet Protocol (IP) address by using the Kovter's payload.
Source: http://news.softpedia.com/news/kovter-malware-victims-were-secret-zombies-in-the-proxygate-proxy-network-499252.shtml

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

Nothing to report

Commercial Facilities Sector

16. *January 22, KABC 7 Los Angeles* – (California) **Fire destroys strip mall in Boyle Heights.** A strip mall housing several businesses in Boyle Heights was heavily damaged January 22 after a fire started from a gas leak inside a laundromat store, causing the front of the structure to collapse. Over 75 firefighters contained the incident and no injuries were reported.
Source: http://abc7.com/news/boyle-heights-strip-mall-damaged-by-fire/1169401/

17. *January 22, WUSA 9 Washington, D.C.* – (Maryland) **More than 20 displaced in Hyattsville apartment fire.** An official from Prince George's County Fire Department reported that 26 residents from a Hyattsville apartment complex were displaced and 15 apartment units were damaged following a January 22 fire. The total amount of damages was unknown and no injuries were reported.
Source: http://www.wusa9.com/story/news/local/maryland/2016/01/22/more-than-20-displaced-hyattsville-apartment-fire/79157610/

18. *January 22, Savannah Morning News* – (Georgia) **Damaged sprinkler system forces evacuation at Sustainable Fellwood apartments.** The Sustainable Fellwood apartment building in Savannah sustained extensive damage and prompted about 60 residents to evacuate the complex January 21 after the sprinkler system had failed due to a damaged water pipe. The building's electrical service will be curtailed until repairs and inspections are complete.
Source: http://savannahnow.com/latest-news/2016-01-22/damaged-sprinkler-system-forces-evacuation-sustainable-fellwood-apartments#

19. *January 21, KABC 7 Los Angeles* – (California) **13 cars damaged in carport fire at Torrance apartment complex.** A January 21 carport fire at the Shamrock Apartments in Torrance, California, damaged 30 parking spaces and potentially totaled 13 vehicles. Officials reportedly believe arson may be the cause of the incident, but are further investigating the cause.
Source: http://abc7.com/news/13-cars-damaged-in-torrance-carport-fire/1168605/

For another story, see item **3**

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