# Daily Open Source Infrastructure Report
## 10 December 2014

## Top Stories

- Officials are investigating after 6 people were killed when an executive jet crashed into a Gaithersburg, Maryland home December 8 and burst into flames, destroying 2 homes and damaging 3 others in the neighborhood. – *Reuters: Chicago Tribune* (See item **7**)

- Repairs to a main break in Annapolis, Maryland, took more than 12 hours after it failed due to external corrosion December 6 and released an estimated 89,000 gallons of wastewater. – *WBAL 1090 AM Baltimore* (See item **13**)

- Kaspersky Lab researchers identified a piece of malware targeting Linux systems associated with the Turla advanced persistent threat (APT) group (also known as Uroburos or Snake) that is based on the cd00r proof-of-concept backdoor. – *Securityweek* (See item **18**)

- The Association of National Advertisers and researchers with White Ops found that around 25 percent of video ads and 11 percent of display ads online are viewed by automated bots set up by cyber criminals to inflate Web site audiences. – *Reuters* (See item **19**)

---

### 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. *December 8, U.S. Environmental Protection Agency* – (Alaska) **North Slope fuel distributor violated oil spill prevention and response safety rules.** The U.S. Environmental Protection Agency (EPA) reached a settlement December 8 with NANA Oilfield Services, Inc., in which the company will pay a $37,500 penalty for violating federal oil spill prevention and response rules at its Deadhorse, Alaska fuel storage and distribution center after the EPA found several violations of the Clean Water Act at the site.
Source: http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/8498b29166bade6785257da80083112d

[Return to top]

## Chemical Industry Sector

Nothing to report

[Return to top]

## Nuclear Reactors, Materials, and Waste Sector

Nothing to report

[Return to top]

## Critical Manufacturing Sector

2. *December 9, Reuters* – (National) **Hyundai recalls 42,925 sedans in U.S. for possible brake light issue.** Hyundai announced a recall of 42,925 model year 2009-2011 Genesis and 2011 Equus vehicles in the U.S. due to the potential for a circuit failure that could cause affected vehicles' brake lights to fail to illuminate.
Source: http://www.reuters.com/article/2014/12/09/us-hyundai-motor-recall-idUSKBN0JN1G820141209

[Return to top]

## Defense Industrial Base Sector

Nothing to report

[Return to top]

## Financial Services Sector

3. *December 9, Bloomberg News* – (International) **Deutsche Bank sued by U.S. over**

**alleged tax scheme.** Federal charges were filed against Deutsche Bank December 8 seeking $190 million in taxes, interest, and penalties for the bank's alleged use of three underfunded shell companies to evade U.S. taxes.
Source: http://www.bloomberg.com/news/2014-12-08/deutsche-bank-sued-by-u-s-over-alleged-tax-scheme.html

4. *December 8, Reuters* – (Massachusetts) **TD Bank settles Massachusetts data breach probe, to pay $625,000.** TD Bank agreed December 8 to a settlement with the State of Massachusetts to pay $625,000 and improve security practices to resolve a probe of a 2012 data breach that exposed the personal information of more than 260,000 customers. The incident was caused by the loss of unencrypted back-up tapes in March 2012 and Massachusetts officials stated that the bank was too slow in reporting the breach to authorities in October.
Source: http://www.reuters.com/article/2014/12/08/torontodominion-massachusetts-settlement-idUSL1N0TS1H320141208

5. *December 8, Cleveland Plain Dealer* – (Ohio) **Federal fraud charges filed against Copley man for $17 million Ponzi scheme with 70 victims.** A Copley Township man who was a co-owner and operator of KGTA Petroleum Ltd., was charged December 8 for allegedly operating the company as a Ponzi scheme, defrauding 70 investors of around $17 million between 2010 and 2014. The man and others, including three PrimeSolutions Securities Inc. representatives, also allegedly failed to file appropriate documentation with the U.S. Securities and Exchange Commission for the company.
Source: http://www.cleveland.com/court-justice/index.ssf/2014/12/federal_fraud_charges_filed_ag.html

6. *December 6, Tulsa World* – (National) **Former Arrow CEO indicted on 23 counts of bank, tax fraud.** The former CEO of nationwide trucking company Arrow Trucking Co., pleaded guilty December 5 in federal court in Texas for allegedly conspiring with others to defraud the Internal Revenue Service and a Utah bank of $24 million in a fraud and tax evasion scheme that operated in 2009. The former CFO of the company previously pleaded guilty December 4 to tax fraud and bank fraud charges.
Source: http://www.tulsaworld.com/news/investigations/former-arrow-ceo-doug-pielsticker-indicted-on-counts-of-bank/article_3ed83e3a-a1ff-5758-b080-e3b6e8928a03.html

For another story, see item **20**

## Transportation Systems Sector

7. *December 9, Reuters; Chicago Tribune* – (Maryland) **Mom, children among 6 dead after jet crashes into Maryland home.** Officials are investigating after the pilot, 2 passengers, and 3 others were killed when an executive jet crashed into a Gaithersburg, Maryland home December 8 and burst into flames. The fire destroyed two homes and damaged three others in the neighborhood.

Source:

8. *December 9, Associated Press; WAVY 10 Portsmouth* – (North Carolina) **NC 12 reopened after Nor'easter flooding, roads narrowed.** The North Carolina Department of Transportation reopened NC 12 in Rodanthe December 9 after closing the roadway December 8 due to flooding. Officials will keep both lanes narrowed through December 11 due to sand and standing water.
Source: http://wavy.com/2014/12/08/nc-12-reopened-after-noreaster-flooding/

9. *December 8, Charleston Daily Mail* – (West Virginia) **Fort Hill Bridge rollover crash kills teen driver.** Authorities are investigating after Interstate 64 in Charleston, West Virginia, was closed for 2 hours December 6 due to a rollover accident that left one person dead and a passenger injured.
Source: http://www.charlestondailymail.com/article/20141208/DM02/141209301/1277

For additional stories, see items **6** and **26**

[Return to top]

## Food and Agriculture Sector

10. *December 8, Jamestown Sun* – (North Dakota) **Colfax grain elevator destroyed by fire.** A Colfax Farmers Elevator Inc. grain elevator in Richland County and the offices attached to it were completely destroyed December 6 when a fire broke out and caused the structure to collapse. Operations were halted until further notice while crews investigated the blaze which also damaged an adjacent grain bin and much of the bins' contents.
Source: http://www.jamestownsun.com/content/colfax-grain-elevator-destroyed-fire

11. *December 6, Orange County Register* – (California) **Firefighters battle blaze near San Juan Capistrano polo ground for hours.** Firefighters responded December 6 to the San Juan Capistrano polo fields in Orange County after a fire broke out inside a hay-filled building that houses Blenheim EquiSports Management Company. The blaze caused about $200,000 in damage to the structure and $300,000 in damage to its contents, which included hundreds of bales of hay, farm equipment, and other pieces of machinery.
Source: http://www.ocregister.com/articles/blaze-644464-juan-firefighters.html

[Return to top]

## Water and Wastewater Systems Sector

12. *December 8, Panama City News Herald* – (Florida) **Boil water notice issued for eastern PCB rescinded.** A boil water advisory issued for several areas in Panama City Beach was lifted December 8 after being issued December 5 when the Panama City Beach Utilities water supply experienced a temporary loss in pressure due to a main

break. Service was restored after the break was repaired.
Source: http://www.newsherald.com/news/crime-public-safety/boil-water-notice-issued-for-eastern-pcb-rescinded-1.409822

13. *December 7, WBAL 1090 AM Baltimore* – (Maryland) **Wastewater overflow reaches Chesapeake Bay.** Repairs to a 10-inch main break in Annapolis, Maryland, took more than 12 hours after it failed due to external corrosion December 6 and released an estimated 89,000 gallons of wastewater. Crews recovered nearly 72,000 gallons of the overflow while approximately 17,000 gallons reached Chesapeake Bay.
Source: http://www.wbal.com/article/111316/2/wastewater-overflow-reaches-chesapeake-bay

## Healthcare and Public Health Sector

14. *December 9, KFOR 4 Oklahoma City* – (Oklahoma) **Man arrested after three nurses, security guard attacked with knife at OKC hospital.** Police arrested a suspect after he allegedly entered the emergency room of Deaconess Hospital in Oklahoma City and stabbed two nurses with a knife December 9. A third nurse and security guard also suffered injuries in the attack and the suspect was found and apprehended by authorities after he barricaded himself in a visiting room at the hospital.
Source: http://kfor.com/2014/12/09/police-two-nurses-stabbed-at-okc-hospital/

For another story, see item **18**

## Government Facilities Sector

15. *December 9, Oklahoma City Oklahoman* – (Oklahoma) **Officials report breach to OU nursing college's web server.** Officials with the University of Oklahoma Health Sciences Center reported December 8 that a server at its College of Nursing was compromised, potentially enabling unauthorized access to the personal information of an unknown amount of students who applied to or attended the College of Nursing from 2005 to the present. The university discovered the breach October 20 and worked to recover the system November 3.
Source: http://newsok.com/officials-report-breach-to-ou-nursing-colleges-web-server/article/feed/769937

16. *December 8, WCBS 2 New York City; Associated Press* – (New York) **6 charged, including 2 former Islip town officials, in illegal-dumping probe on Long Island.** Six individuals were charged, including the former Islip town parks commissioner and his former secretary, following an investigation into the alleged illegal dumping of more than 1,700 truckloads of debris at four Long Island sites. Investigators found about 50,000 tons of debris tainted with asbestos, pesticides, and other material at Islip-owned Roberto Clemente Park in Brentwood and determined the individuals were

allegedly hauling the demolition debris from New York City in order to avoid costly legal disposal.
Source: http://newyork.cbslocal.com/2014/12/08/6-charged-in-illegal-dumping-probe-on-long-island/

17. *December 8, Moscow-Pullman Daily News* – (Idaho) **No bomb at MHS.** Moscow High School in Idaho was evacuated and classes were dismissed December 8 due to a bomb threat. Police cleared the scene after nothing suspicious was found and continue to investigate the threat.
Source: http://dnews.com/breaking_news/article_3762dbd6-7f03-11e4-87ca-bf5cd329ab74.html

For another story, see item **18**

## Emergency Services Sector

Nothing to report

## Information Technology Sector

18. *December 9, Securityweek* – (International) **Newly discovered 'Turla' malware targets Linux systems.** Kaspersky Lab researchers identified a piece of malware targeting Linux systems associated with the Turla advanced persistent threat (APT) group (also known as Uroburos or Snake) that is based on the cd00r proof-of-concept backdoor and is capable of hidden network communications, remote management, and arbitrary remote command execution. Previous versions of Turla malware have targeted Windows systems in government agencies, military groups, educational institutions, pharmaceutical companies, and other targets in more than 45 countries.
Source: http://www.securityweek.com/newly-discovered-turla-malware-targets-linux-systems

19. *December 9, Reuters* – (International) **Fraud from bots represents a loss of $6 bln in digital advertising.** The Association of National Advertisers and researchers with White Ops released a report December 9 which found that around 25 percent of video ads and 11 percent of display ads online are viewed by automated bots set up by cyber criminals to inflate Web site audiences. The researchers stated that such fraud could cost advertisers an estimated $6.3 billion in the next year.
Source: http://www.reuters.com/article/2014/12/09/advertising-fraud-study-idUSL1N0TS19220141209

20. *December 9, Softpedia* – (International) **POODLE attack also affects some TLS implementations.** A researcher with Google reported that certain implementations of Transport Layer Security (TLS) with an SSL 3.0 decoding function can be exploited

through POODLE attacks to decrypt sensitive information. The researcher identified the vulnerability in older versions of Network Security Services (NSS) as well as in Web sites administered by Bank of America with load balancing devices from A10 Networks and F5 Networks.
Source: http://news.softpedia.com/news/POODLE-Attack-Also-Affects-Some-TLS-Implementations-466944.shtml

21. *December 9, Help Net Security* – (International) **Info on millions of AliExpress customers could have been harvested due to site flaw.** A security researcher identified and reported a flaw in the AliExpress online marketplace that could have allowed a logged-in user to exploit an insecure direct object reference vulnerability to view other users' names, addresses, and phone numbers. Alibaba, parent company of AliExpress, closed the vulnerability after the researcher's report.
Source: http://www.net-security.org/secworld.php?id=17741

22. *December 8, Softpedia* – (International) **Yik Yak flaw de-anonymizes user, allows control over account.** SilverSky researchers identified and reported a vulnerability in the Yik Yak anonymous social media platform for iOS that could allow an attacker to discover the identity of a user and take over their account due to the Flurry advertising tool sending the app's secure ID used by the app in the place of a password without encryption. The researchers reported the issue to Yik Yak and a patch was released in December.
Source: http://news.softpedia.com/news/Yik-Yak-Flaw-De-anonymizes-User-Allows-Control-Over-Account-466877.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

[Return to top]

## Communications Sector

23. *December 6, Las Vegas Review-Journal* – (Nevada) **Channel 13 fined over so-called 'special reports'.** Journal Broadcasting Corp., was ordered to pay a $115,000 penalty by the U.S. Federal Communications Commission (FCC) December 6 in a settlement after its television station KTNV 13 Las Vegas represented paid ads as "special reports" in 2009 failing to disclose the reports were actually paid advertisements, which violated the FCC's sponsorship identification rule.
Source: http://www.reviewjournal.com/news/las-vegas/channel-13-fined-over-so-called-special-reports

[Return to top]

## Commercial Facilities Sector

24. *December 9, Richmond Times-Dispatch* – (Virginia) **Gas leak forces evacuation, detours around S. Richmond apartment building.** Around 150 residents were evacuated from the Hopper Lofts apartment building in south Richmond December 9 due to a gas leak. City utilities officials reported that residents were expected to be allowed back into their apartments about 8 hours from the time the leak was reported.
Source: http://www.timesdispatch.com/news/local/gas-leak-forces-evacuation-detours-around-s-richmond-apartment-building/article_86958708-c984-5b07-8f83-52e1f30fd791.html

25. *December 8, WCBS 2 New York City; Associated Press* – (New Jersey) **Dozens displaced after 4-alarm fire rips through 3 buildings in Newark.** A 4-alarm fire December 8 tore through 3 buildings in Newark that house street-level stores and apartments, causing a partial structure collapse. Two firefighters were injured and 29 residents were displaced by the fire.
Source: http://newyork.cbslocal.com/2014/12/08/dozens-displaced-after-4-alarm-fire-rips-through-3-buildings-in-newark/

26. *December 8, Los Angeles Times* – (California) **L.A. fire: Damage to 110 Freeway estimated at $1.5 million, at least.** Authorities reported that a December 8 fire that engulfed the under-construction Da Vinci apartment building in Los Angeles caused an estimated $10 million in structural damage to the development, while nearby buildings including a government building were also damaged. A portion of the 110 Freeway that runs adjacent to the structure suffered an estimated $1.5 million in damage to road signs, wooden guardrails, rubber sealant, and metal posts.
Source: http://www.latimes.com/local/lanow/la-me-ln-la-fire-damage-costs-20141208-story.html

27. *December 7, Kingston Daily Freeman* – (New York) **Town of Ulster Walmart, other stores reopen after threat, evacuation, police say.** At least three businesses located at a shopping plaza in the Town of Ulster were evacuated December 6 while authorities investigated a threatening call that was phoned in to a Walmart store at the shopping complex. The stores reopened after about 2 hours following a police search that cleared the scene.
Source: http://www.dailyfreeman.com/general-news/20141206/town-of-ulster-walmart-other-stores-reopen-after-threat-evacuation-police-say

[Return to top]

## Dams Sector

Nothing to report

[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.