Homeland Security

# Daily Open Source Infrastructure Report 19 January 2016

## Top Stories

- The Office of Inspector General released a report January 14 following its audit of the Security Operations Center (SOC) that revealed cyberattacks against U.S. power plants grew by 18 percent from 2013 – 2014. – *Softpedia* (See item **3**)
- JetBlue officials reported January 14 that a Verizon data center outage affected its online check-in system, flight booking, and JetBlue mobile application and delayed or cancelled flights leaving from three major international airports. – *CNBC* (See item **10**)
- Hyatt Hotel officials reported January 15 that its payment processing system was compromised and affected 250 international hotels after an investigation revealed a malicious malware was installed onto its systems. – *SecurityWeek* (See item **21**)
- Officials reported that up to 500 people were evacuated from two Manhattan office buildings January 14 after an 8-inch gas main ruptured and leaked chemicals into the air. – *WNBC 4 New York City* (See item **22**)

## Fast Jump Menu

**PRODUCTION INDUSTRIES**

**SUSTENANCE and HEALTH**

**SERVICE INDUSTRIES**

**FEDERAL and STATE**

## Energy Sector

1. *January 14, SecurityWeek* – (National) **Oil and gas industry increasingly hit by cyber-attacks: Report.** Researchers from Tripwire Inc., released a report stating that 82 percent of oil and gas industry organizations have experienced an increase in successful cyberattacks over the past 12 months, with a 50 to 100 percent increase in attacks within November 2015.
   Source: http://www.securityweek.com/oil-and-gas-industry-increasingly-hit-cyber-attacks-report

2. *January 14, KFOR 4 Oklahoma City* – (Oklahoma) **Fracking fire damage totals almost $50 million.** A January 13 fire at the Continental Resources oil site in Grady County caused $50 million in damages, destroyed 22 company vehicles, and prompted fire crews to remain on site for about 4 hours while they contained the incident. No injuries were reported and officials are investigating the incident.
   Source: http://kfor.com/2016/01/14/fracking-fire-damage-totals-almost-50-million/

## Chemical Industry Sector

Nothing to report

## Nuclear Reactors, Materials, and Waste Sector

3. *January 15, Softpedia* – (International) **Nuclear Power Plants from all over the world are vulnerable to cyberattacks.** The Office of Inspector General released a report following its audit of the Security Operations Center (SOC) that revealed cyberattacks against U.S. power plants grew by 18 percent from 2013 – 2014 and that the SOC did not meet the necessary quality control criteria to continue its operations without implementing corrective action plans. In addition, the Nuclear Threat Initiative released a similar report revealing that 20 international countries, using extensive nuclear energy systems were vulnerable to cyberattacks due to their low cybersecurity protocols.
   Source: http://news.softpedia.com/news/nuclear-power-plants-from-all-over-the-world-are-vulnerable-to-cyberattacks-498955.shtml

## Critical Manufacturing Sector

Nothing to report

## Defense Industrial Base Sector

See item **9**

## Financial Services Sector

4. *January 14, U.S. Securities and Exchange Commission* – (National) **SEC Charges Goldman Sachs with improper securities lending practices.** Goldman, Sachs & Co.

agreed to pay the U.S. Securities and Exchange Commission (SEC) $15 million in penalties January 14 to settle charges that the company inaccurately recorded the firm's locates log and violated Federal regulations in its securities lending practices by improperly providing locates to customers without performing an appropriate review of the securities to be located, leading customers to engage in illegal short selling sales, among other charges.
Source: http://www.sec.gov/news/pressrelease/2016-9.html

5. *January 14, U.S. Securities and Exchange Commission* – (Ohio) **SEC charges State Street for pay-to-play scheme.** The U.S. Securities and Exchange Commission announced January 14 that State Street Bank and Trust Company agreed to a $12 million settlement over allegations that the company conducted a pay-to-play scheme in which the company's former senior vice president agreed to make illicit cash payments and political campaign contributions to Ohio's deputy treasurer in order to win sub-custodian contracts to service Ohio pension funds.
Source: http://www.sec.gov/news/pressrelease/2016-8.html

6. *January 14, U.S. Attorney's Office, Eastern District of Virginia* – (Virginia) **Federal jury convicts ringleader of bank fraud and identity theft scheme.** A man from Virginia was convicted January 13 by a Federal jury for 1 count of conspiracy to commit bank fraud, 19 counts of bank fraud, and 4 counts of aggravated identity theft after an investigation revealed he was the organizer of a nationwide bank fraud and identity theft scheme that targeted banks and individuals, and opened numerous checking, credit, and personal line accounts using the stolen identities of his victims.
Source: http://www.justice.gov/usao-edva/pr/federal-jury-convicts-ringleader-bank-fraud-and-identity-theft-scheme

7. *January 13, Reuters* – (Philadelphia) **U.S. jury finds ex-Capital One analyst liable in insider trading case.** A Federal jury convicted a former Capital One Financial Corp analyst January 13 on civil charges that he engaged in insider trading by using non-public sales data, gathered by the credit card company, to buy and sell stocks in advance while disguising the non-public sales data as material data. The traded information gave the man a significant advantage and earned him $1.5 million in trade sales.
Source: http://www.reuters.com/article/us-sec-capitalone-insidertrading-idUSKCN0UR2KR20160113

8. *January 13, San Diego Union-Tribune* – (California) **'Hipster Bandit' robs forth bank.** Authorities are searching January 13 for a man dubbed the "Hipster Bandit" after he allegedly robbed four banks in San Diego including his most recent robbery at a Wells Fargo Bank branch January 9 in which the suspect slipped a note to the teller and demanded specific denominations before leaving with the stolen funds.
Source: http://www.sandiegouniontribune.com/news/2016/jan/13/hipster-bandit-robs-fourth-bank/

## Transportation Systems Sector

9. *January 15, CNN* – (Hawaii) **Military aircraft collide in Hawaii; search on for survivors.** Officials are investigating the cause of a helicopter collision after two CH-53 helicopters collided January 14 off the coast of Oahu, leaving 12 U.S. Marines missing at sea.
Source: http://www.cnn.com/2016/01/15/us/hawaii-military-aircraft-collision/index.html

10. *January 14, CNBC* – (National) **Verizon outage disrupts JetBlue service nationwide.** JetBlue officials reported January 14 that a Verizon data center outage affected its online check-in system, flight booking, and JetBlue mobile application and delayed or cancelled flights leaving from Los Angeles International Airport, John F. Kennedy International Airport, and Logan International Airport, among other airports. Verizon officials reported that the data center power was restored.
Source: http://www.cnbc.com/2016/01/14/jetblue-experiencing-intermittent-network-issues-due-to-data-center-power-outage.html

11. *January 14, Biloxi Sun Herald* – (Mississippi) **607 reopens after cleanup of 300-gallon corrosive spill.** Mississippi 607 reopened January 14 after being closed for more than 24 hours while crews cleaned up a corrosive chemical spill following a January 13 accident involving an overturned semi-truck.
Source: http://www.sunherald.com/news/local/traffic/article54666960.html

12. *January 14, WHAS 11 Louisville* – (Kentucky) **Woman killed in crash on Joe Prather Hwy.** Joe Prather Highway in Hardin and Meade County was closed for several hours January 14 while crews worked to clear the wreckage from a fatal two-vehicle crash that killed one driver and sent the other to the hospital with non-life-threatening injuries.
Source: http://www.whas11.com/story/news/traffic/accident-construction/2016/01/14/1-killed-another-injured-after-crash-joe-prather-hwy/78793634/

13. *January 14, Davidson Civitas Media* – (Ohio) **2-car crash near New Hampshire shuts down U.S. 33.** U.S. 33 was shut down for more than two hours January 14 while crews worked to clear the wreckage from a two-vehicle crash that sent two drivers to the hospital.
Source: http://limaohio.com/news/161152/2-car-crash-near-new-hampshire-shuts-down-u-s-33

## Food and Agriculture Sector

Nothing to report

## Water and Wastewater Systems Sector

14. *January 14, KNSD 39 San Diego* – (California) **Sewage spill contaminates more of**

**Mission Bay.** Officials expanded the water closure of Mission Bay in San Diego to include additional northern areas January 14 after collected water samples revealed contaminated water had traveled north following a broken mail sewer line that leaked 108,000 gallons of polluted water into the Mission Bay.
Source: http://www.nbcsandiego.com/news/local/Sewage-Spill-Contaminates-More-of-Mission-Bay--365364491.html

For another story, see item **16**

## Healthcare and Public Health Sector

Nothing to report

## Government Facilities Sector

15. *January 15, Salisbury Daily Times* – (Maryland) **Worchester schools evacuating after bomb threat made.** A bomb threat prompted all Worcester County public schools to be evacuated and closed January 15 after Parkside High School in Salisbury received a phoned-in bomb threat, which indicated there were active bombs in all the school district buildings. Officials are investigating the incidences.
Source: http://www.delmarvanow.com/story/news/local/maryland/2016/01/15/worcester-schools-evacuating/78850222/

16. *January 15, Associated Press* – (Maryland) **3 Baltimore schools closed due to water main break.** Three Baltimore schools including Gwynns Falls Elementary, ConneXions School for the Arts, and Maryland Academy of Technology and Health Services were closed January 15 due to a 36-inch water main break that ruptured January 13. Crews were working to drain thousands of gallons of water from the water main to access and repair the damage.
Source: http://www.beaumontenterprise.com/news/article/3-Baltimore-schools-closed-due-to-water-main-break-6760991.php

## Emergency Services Sector

Nothing to report

## Information Technology Sector

17. *January 15, Help Net Security* – (International) **Flaw allows malicious OpenSSH servers to steal users' private SSH keys.** Researchers from Qualys reported that two vulnerabilities including an Information Disclosure flaw were found in the OpenSSH implementation of the secure shell (SSH) protocol that can allow an attacker to pose as an owner of the SSH keys and extract users' private cryptographic keys through the default client code that can be tricked into leaking client memory to the server.
Source: http://www.net-security.org/secworld.php?id=19334

18. *January 15, SecurityWeek* – (International) **Alleged author of MegalodonHTTP malware arrested.** Norwegian officials arrested an individual suspected of authoring the MegalodonHTTP malware that powers distributed denial-of-service (DDoS) botnets internationally after police arrested five men on suspicion of possessing, using, and selling malware. Authorities reported that the malware's moniker is no longer active or doing business once the man was arrested.
Source: http://www.securityweek.com/alleged-author-megalodonhttp-malware-arrested

19. *January 15, SecurityWeek* – (International) **McAfee Application Control Flaws expose critical infrastructure: Researchers.** A researcher from SEC Consult discovered a series of low level vulnerabilities in McAfee's Application Control product that can be exploited to bypass application whitelisting protection and gain arbitrary code execution through various techniques, which can be leveraged to cause denial-of-service (DoS) conditions to overwrite whitelisted applications once code execution is achieved.
Source: http://www.securityweek.com/mcafee-application-control-flaws-expose-critical-infrastructure-researchers

20. *January 14, InfoWorld* – (International) **Google's Go upgrade fixes bug that could leak RSA private key.** Google released an update to its programming language, Go 1.5.3, patching a security issue that can affect RSA computations in cryto/rsa used by crypto/tls and potentially leak their RSA private key on TLS servers with 32-bit systems.
Source: http://www.computerworld.com/article/3023034/application-development/googles-go-upgrade-fixes-bug-that-could-leak-rsa-private-key.html#tk.rss_security

For another story, see item **21**

### 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

21. *January 15, SecurityWeek* – (International) **Card breach affects 250 Hyatt Hotels worldwide.** Hyatt Hotel officials reported that its payment processing system used at Hyatt-managed locations including restaurants, golf shops, and spa resorts, was compromised and affected about 250 hotels internationally after an investigation revealed a malicious malware was installed onto its systems that collected cardholder

names, card numbers, expiration dates, and internal verification codes. The hotel is offering one year of free fraud protection to those affected via CSID.
Source: http://www.securityweek.com/card-breach-affects-250-hyatt-hotels-worldwide

22. *January 14, WNBC 4 New York City* (New York) **Gas leak prompts evacuation of Manhattan buildings.** Officials reported that up to 500 people were evacuated from two Manhattan office buildings January 14 after an 8-inch gas main ruptured and leaked chemicals into the air. Authorities shut off the gas and are working to repair the leak.
Source: http://www.nbcnewyork.com/news/local/Gas-Leak-Con-Edison-Evacuation-Manhattan--365335631.html

## Dams Sector

Nothing to report

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.