Daily Open Source Infrastructure Report
16 January 2013

Top Stories

- Recently, malware attacks at two energy companies infiltrated critical networks, highlighting the need for companies to adhere to best practices in protecting their networks from cyber attacks. A report from the Industrial Control Systems Cyber Emergency Response Team suggested cleaning USB drives after each use, maintaining system backups, and other methods as a way to mitigate threats against industrial control systems. – *Threatpost* (See item **1**)
- Two illegal immigrants from Romania were arrested in Englewood for allegedly running an ATM skimming operation that stole more than $1 million from customers' accounts. – *Bergen County Record* (See item **5**)
- A water treatment plant in Jefferson County experienced a major mechanical failure over the January 12 weekend that allowed 95 million gallons of wastewater mixed with storm water to flood the area. – *Louisville Courier Journal* (See item **13**)
- The Whites Creek school remained closed January 15 after a carbon monoxide leak January 14 sent 40 students to the hospital. – *WTVF 5 Nashville* (See item **19**)

Fast Jump Menu

Energy Sector

1. *January 14, Threatpost* – (National) **Malware infects two power plants lacking basic security controls.** Recently, malware attacks at two energy companies infiltrated critical networks, highlighting the need for companies to adhere to best practices in protecting their networks from cyber attacks. A report from the Industrial Control Systems Cyber Emergency Response Team suggested cleaning USB drives after each use, maintaining system backups, and other methods as a way to mitigate threats against industrial control systems.
   Source: http://threatpost.com/en_us/blogs/malware-infects-two-power-plants-lacking-basic-security-controls-011413

[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

Nothing to report

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

2. *January 15, Las Vegas Sun* – (Nevada) **Las Vegas lawyer pleads to mortgage fraud scheme in valley.** A Las Vegas lawyer entered a guilty plea for charges relating to his role in a mortgage fraud scheme that defrauded lending institutions of $30 million.
   Source: http://www.lasvegassun.com/news/2013/jan/14/las-vegas-lawyer-pleads-mortgage-fraud-scheme/

3. *January 15, Palm Harbor Patch* – (Florida) **Palm Harbor 'Bank Bag Bandit' pleads guilty.** The man known as the "Bank Bag Bandit" pleaded guilty the week of January 7 to five armed robberies in three Florida counties.
   Source: http://palmharbor.patch.com/articles/palm-harbor-bank-bag-bandit-pleads-guilty

4. *January 14, Bloomberg News* – (National) **JPMorgan ordered to fix controls, pay practices after Whale bet.** The Federal Reserve and the Office of the Comptroller of the Currency ordered JPMorgan Chase & Co. to increase its trading oversight and use better anti-money laundering practices after significant deficiencies in risk management were cited by regulators.
   Source: http://www.businessweek.com/news/2013-01-14/jpmorgan-s-whale-trade-subject-of-occ-order-to-fix-risk-controls

5. *January 14, Bergen County Record* – (New Jersey) **Two men, natives of Romania, are arrested in ATM scam that netted more than $1 million.** Two illegal immigrants from Romania were arrested in Englewood for allegedly running an ATM skimming operation that stole more than $1 million from customers' accounts.
   Source: http://www.northjersey.com/englewood/Two_men_natives_of_Romania_are_arrested_in_ATM_scam_that_netted_more_than_1_million.html

For another story, see item **18**

[Return to top]

Transportation Sector

6. *January 15, Los Angeles Times* – (California) **Big rig accident closes 5 Freeway near Elysian Park.** A truck crashed and caught fire on 5 Freeway near Elysian Park January 14, blocking traffic in both directions for at least 6 hours, according to the California Highway Patrol.
   Source: http://latimesblogs.latimes.com/lanow/2013/01/big-rig-accident-closes-i-5-near-glendale-freeway-.html

7. *January 15, Associated Press* – (Washington) **Fatal crash on bridge near Oakville.** A Washington State Patrol trooper said one person was killed and three were injured in a crash January 15 on Highway 12 in Grays Harbor County, blocking the highway for 4 hours.
   Source: http://www.sfgate.com/news/crime/article/Fatal-crash-on-bridge-near-Oakville-4195324.php

8. *January 15, Associated Press* – (Mississippi) **State of emergency declared over Miss. ice storm.** The Mississippi governor declared a state of emergency after numerous Mississippi counties experienced ice storms and faced flooding dangers.
   Source: http://www.sfgate.com/news/article/Ice-storm-causes-problems-for-parts-of-Miss-4192924.php

9. *January 15, Lafayette Advertiser* – (Louisiana) **United Airlines jet diverted from Lafayette.** A United Airlines aircraft that departed Houston en route to Lafayette, Louisiana, had to make a detour to Baton Rouge after Lafayette Regional Airport reported that a part of the landing system was out of commission due to construction.
Source: http://www.theadvertiser.com/article/20130115/BUSINESS/130115016/United-Airlines-jet-diverted-from-Lafayette?nclick_check=1

10. *January 14, San Bernadino Sun* – (California) **Wind, icy roads cause problems throughout Inland Empire.** High winds and ice storms caused several crashes in the San Bernardino area, leading to freeway shutdowns.
Source: http://www.sbsun.com/news/ci_22369196/wind-icy-roads-cause-problems-throughout-inland-empire

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

11. *January 15, Food Safety News* – (Missouri; Iowa) **Missouri artisan cheese recalled for E. coli risk.** Homestead Creamery of Jamesport, Missouri, voluntarily recalled a batch of its Flory's Favorite cheese due to possible contamination of Shiga-Toxin producing E.coli.
Source: http://www.foodsafetynews.com/2013/01/missouri-artisan-cheese-recalled-for-e-coli-risk/#.UPVUHx2Cm58

12. *January 15, Associated Press* – (National) **Zaxby's warns customers of potential fraud.** Zaxby's Franchising Inc. officials found suspicious computer files that may have resulted in unauthorized access to credit and debit card information affecting over 100 stores nationwide.
Source: http://www.nbc12.com/story/20589322/zaxbys-warns-customers-of-potential-fraud

[Return to top]

Water Sector

13. *January 14, Louisville Courier Journal* – (Kentucky) **95 million gallons of storm and wastewater spill into Louisville creeks after treatment plant failure.** A water treatment plant in Jefferson County experienced a major mechanical failure over the January 12 weekend that allowed 95 million gallons of wastewater mixed with storm water to flood the area.

Source: http://www.courier-journal.com/article/20130114/NEWS01/301140051/95-million-gallons-storm-wastewater-spill-into-Louisville-creeks-after-treatment-plant-failure

14. *January 14, KELO 11 Sioux Falls* – (South Dakota) **Alcester to shut off water on Tuesday.** Workers in Alcester failed to find the source of a leak, leaving the town without water and schools closed January 15.
Source: http://www.keloland.com/newsdetail.cfm/alcester-to-shut-off-water-on-tuesday/?id=142477

15. *January 14, Charleston Gazette* – (West Virginia) **Water advisories issued for Mount Hope, Danese.** The city of Mount Hope was placed under a boil water advisory January 14 after a water main break.
Source: http://sundaygazettemail.com/News/201301140121

[Return to top]

Public Health and Healthcare Sector

16. *January 15, Associated Press* – (National) **St. Jude Medical gets FDA warning about problems at Sylmar plant.** The Food and Drug Administration warned St. Jude about production inconsistencies on their implantable heart defibrillators, noting several quality-control problems. St. Jude said they are correcting the problems noted by the government.
Source: http://www.latimes.com/business/la-fi-fda-st-jude-20130115,0,5025416.story

17. *January 14, Healthcare Finance News* – (National) **3 strategies for strengthening internal data security practices.** The Vice President of Public Sector Sales and Marketing at Dell identified three elements that may mitigate risk to healthcare IT systems: Two-factor identification, identity of service, and least privileges.
Source: http://www.healthcarefinancenews.com/news/3-strategies-strengthening-internal-data-security-practices

18. *January 8, Mount Pleasant Daily Tribune* – (Texas) **Former State HHS employee charged with identity theft; hundreds may be impacted.** Authorities have arrested a former employee of the Texas Department of Health and Human Service and accused her of using identity theft for personal gain after numerous Texas Department of Health and Human Service customers filed identify-theft complaints with the Titus County Sheriff's Office.
Source: http://www.dailytribune.net/news/article_960984e0-5959-11e2-84e9-001a4bcf887a.html

[Return to top]

Government Facilities Sector

19. *January 15, WTVF 5 Nashville* – (Tennessee) **Drexel Academy students treated for carbon monoxide poisoning.** The Whites Creek school remained closed January 15 after a carbon monoxide leak January 14 sent 40 students to the hospital.
Source: http://www.newschannel5.com/story/20585401/drexel-academy-student-treated-for-carbon-monoxide-poisoning

20. *January 14, Associated Press; KTUU 2 Anchorage* – (Alaska) **Man charged with terroristic threat after JBER gate closure.** Anchorage police arrested a man after he threw a suspicious package, while making a threat of possible use of explosives, at the Joint Base Elmendorf-Richardson gate January 14. The base was shut down for 2 hours while authorities examined the package made up of an aerosol spray can, vinegar bottle, and several other materials.
Source: http://www.adn.com/2013/01/14/2752191/suspicious-package-causes-closure.html

For more stories, see items **14** and **18**

[Return to top]

Emergency Services Sector

21. *January 14, Associated Press* – (New Jersey) **NJ firefighter pleads guilty to burning empty home.** A New Jersey firefighter plead guilty January 14 to to setting a vacant home on fire with gasoline he stole from the fire station.
Source: http://www.chron.com/news/crime/article/NJ-firefighter-pleads-guilty-to-burning-empty-home-4193045.php

22. *January 14, Yankton Daily Press & Dakotan* – (South Dakota) **Yankton County Jail escapee captured in Sioux Fall.** A Yankton County Jail inmate that escaped in Fall 2012 was found and taken into custody January 14 in Sioux Falls.
Source:
http://www.yankton.net/articles/2013/01/14/community/doc50f4868614a36741512683.txt

[Return to top]

Information Technology Sector

23. *January 15, Help Net Security* – (International) **Waledac botmasters use Virut malware to build a new botnet.** The botmasters behind the Waledac (also known as Kelihos) botnet have been found by Symantec researchers to be infecting computers by using the Virut botnet in an attempt to rebuild their own botnet. W32.Waledac.D infections have risen, mostly on computers in the U.S.
Source: http://www.net-security.org/malware_news.php?id=2376&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader

24. *January 15, Softpedia* – (International) **Red October cyber espionage campaign relied on Java exploit to infect computers.** Researchers at Seculert analyzed the recently-discovered 'Red October' cyber espionage campaign and found that it had also utilized a Java vulnerability to disseminate malware.
Source: http://news.softpedia.com/news/Red-October-Cyber-Espionage-Campaign-Relied-on-Java-Exploit-to-Infect-Computers-321319.shtml

25. *January 14, Krebs on Security* – (International) **Microsoft issues fix for zero-day IE flaw.** Microsoft released an emergency out-of-band security update to close a critical security vulnerability in Internet Explorer versions 6, 7, and 8 that was recently used in targeted attacks.
Source: http://krebsonsecurity.com/2013/01/microsoft-issues-fix-for-zero-day-ie-flaw/

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: https://www.it-isac.org

[Return to top]

Communications Sector

Nothing to report

[Return to top]

Commercial Facilities Sector

26. *January 15, Rochester Post-Bulletin* – (Minnesota) **Apartment fire leaves 20 without homes.** Firefighters responded to a fire in Rochester January 14 that left 20 residents displaced, sent 5 to the hospital, and caused around $200,000 in damage.
Source: http://www.postbulletin.com/news/local/apartment-fire-leaves-without-homes/article_8286a438-43b4-57cc-899a-ffc89d1a86af.html

27. *January 15, Los Angeles Times* – (California) **Five arrested in connection with robbery at Nordstrom Rack.** A total of five arrests were made in the investigation of a hostage situation in Los Angeles January 10 in which robbers held 14 employees hostage.
Source: http://www.latimes.com/news/local/la-me-0115-nordstrom-rack-arrests-20130115,0,7196344.story

28. *January 15, Hartford Courant* – (Connecticut) **Residents leapt from windows to escape East Hartford apartment fire.** A 3-alarm fire January 15 in Hartford left nine residents and three firefighters injured. A total of 38 units were affected by the fire.

Source: http://www.courant.com/community/east-hartford/hc-east-hartford-three-fire-0115-20130115,0,275538.story

29. *January 15, KHON 2 Honolulu* – (Hawaii) **Roadways reopen in Moiliili following building fire at Marco Polo.** Residents of a 36-story condo were evacuated from a 3-alarm fire January 15.
Source: http://www.khon2.com/news/local/story/Fire-crews-respond-to-Marco-Polo-building-fire-in/hniqhnt3Hk2X6QZlonJJLQ.cspx

30. *January 14, Warrick Publishing* – (Indiana) **Four arrested at Newburgh meth lab.** Four suspects were arrested at a Newburgh apartment complex January 10 after the discovery of two meth labs.
Source: http://www.tristate-media.com/warrick/article_ceb3d7ac-5e6b-11e2-829f-001a4bcf887a.html

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

31. *January 15, Cape Girardeau Southeast Missourian* – (Missouri) **Two of three Birds Point levee crevasses rebuilt.** Construction on two of three levees breached in May 2011 was completed behind schedule as a result of delays due to weather.
Source: http://www.semissourian.com/story/1931138.html

32. *January 14, U.S. Department of Labor* – (Nevada) **US Department of Labor's OSHA finds 58 safety and health violations at Hoover Dam Hydroelectric Power Plant in Boulder City, Nev.** The Hoover Dam Hydroelectric Power Plant was found to be in violation of 8 repeat and 50 serious safety and health violations by the U.S. Department of Labor's Occupational Safety and Health Administration.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=23526

[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) 387-2341
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