



Daily Open Source Infrastructure Report 11 March 2016

Top Stories

- Elevated levels of lead found in water at 30 Newark, New Jersey schools required schools to shut off drinking fountains and post warning signs March 9. – *CNN* (See item [20](#))
- Kaspersky discovered a new trojan reportedly believed to be the most advanced mobile malware yet, dubbed Triada that targets Android operating system (OS) devices. – *SecurityWeek* (See item [25](#))
- Florida-based Rosen Hotels & Resorts Inc., reported March 9 that its payment processing system was compromised which allowed attackers to steal customer data including cardholders’ names, card numbers, and internal verification codes. – *Softpedia* (See item [28](#))
- Approaching rain storms in Bossier City, Louisiana, prompted the evacuation of 3,500 homes March 10, the declaration of a State of emergency in several Louisiana parishes, and the closure of Bossier Parish public schools and Northwestern State University campuses. – *Associated Press* (See item [30](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)

Energy Sector

1. *March 9, Pittsburgh Business Times* – (Pennsylvania) **Beaver County coal-fired plant offline temporarily due to low prices.** FirstEnergy Corp., confirmed March 9 that three coal-fired generating units at the Bruce Mansfield plant in Beaver County were taken offline in February until further notice due to low energy prices. The utility reported that employees are continuing maintenance work at the plant while it remains offline.
Source: <http://www.bizjournals.com/pittsburgh/blog/energy/2016/03/beaver-county-coal-fired-plant-offline-temporarily.html>
2. *March 9, WWBT 12 Richmond* – (Virginia) **Dominion, James River Association agree to wastewater discharge plan.** Dominion Virginia Power and the James River Association announced March 9 that a settlement agreement was reached on discharges of treated waste from coal ash ponds at the utility's Fluvanna County power station requiring Dominion to build and operate a wastewater treatment system at its Bremo Power Station and enhance treatment of the pond water and fish tissue monitoring, while the association agreed to refrain from appealing a wastewater permit issued for the power station.
Source: <http://www.nbc12.com/story/31426572/dominion-james-river-association-agree-to-wastewater-discharge-plan>

For another story, see item [15](#)

Chemical Industry Sector

See item [11](#)

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

3. *March 9, Manchester Journal Inquirer* – (Connecticut) **2 fires inflict heavy damage at Enfield factory.** A March 8 fire that reignited several hours later at the Yankee Casting Co, plant in Enfield, Connecticut, severely damaged seven out of nine building additions and caused significant damage to the roof. The cause of the fire remains under investigation.
Source: http://www.journalinquirer.com/towns/enfield/fires-inflict-heavy-damage-at-enfield-factory/article_3e7e73de-e605-11e5-bfb1-df2572580108.html

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

4. *March 10, Associated Press* – (Alabama; Tennessee) **Alabama car dealers admit bank fraud.** Nashville officials announced March 10 that 2 New Market, Alabama residents pleaded guilty to charges alleging that the pair used their pre-owned car business to defraud 65 financial institutions by seeking multiple loans on over 100 vehicles from different financial institutions by using fraudulently obtained titles as collateral. The scheme caused \$5.9 million in losses over a five year period.
Source: <http://www.wrcbtv.com/story/31433311/alabama-car-dealers-admit-bank-fraud>

5. *March 9, U.S. Securities and Exchange Commission* – (International) **Money returning to investors harmed by unregistered broker.** The U.S. Securities and Exchange Commission (SEC) announced March 9 that Cyprus-based Banc de Binary Ltd., agreed to pay a total of \$11 million to the SEC and Commodity Futures Trading Commission (CFTC) to settle charges that the company, its founder, and three affiliates illegally sold binary options to U.S. investors after the company failed to register as a broker-dealer before communicating directly with U.S. clients via phone, email, and instant messenger chats, and soliciting U.S. customers through YouTube videos, spam emails, and other Internet advertising outlets. A Fair Fund was established to compensate harmed investors and Banc de Binary Ltd., its founder, and its affiliates agreed to be suspended from the securities industry for a year and permanently banned from issuing penny stock offerings.
Source: <https://www.sec.gov/news/pressrelease/2016-42.html>

6. *March 9, Lee's Summit Journal* – (Missouri) **Greenwood man indicted for mortgage fraud scheme.** A Greenwood, Missouri home builder, doing business as Penrod Homes, Inc., was charged March 8 for his role in a scheme to defraud mortgage lenders from May 2005 – June 2007 where he and others allegedly recruited buyers to apply for mortgage loans to purchase 61 homes in Greenwood and Peculiar that later went into foreclosure causing the banks and mortgage companies approximately \$4.5 million in losses, and accepted illegal kickbacks totaling \$1.5 million on 57 of the homes sold.
Source: http://www.lsjournal.com/2016/03/09/137896_greenwood-man-indicted-for-mortgage.html

7. *March 8, Greenville News* – (South Carolina) **Greenville broker indicted in \$3 million Ponzi scam.** A former Greenville, South Carolina broker was indicted on Federal fraud charges March 8 after he allegedly ran a \$2.8 million Ponzi scheme where he advised clients to invest their money into a fictitious company, SG Investment Management, provided investors with bogus earning statements, and returned a portion of the funds to make it appear as though the clients' funds were invested and earning profits between 2000 – 2014.
Source: <http://www.greenvilleonline.com/story/news/crime/2016/03/08/greenville-broker-indicted-3-million-ponzi-scam/81495112/>

8. *March 8, U.S. Attorney's Office, Western District of Kentucky* – (Kentucky) **Louisville attorney charged with wire fraud and money laundering.** The U.S. Attorney's Office in Kentucky announced March 8 that a former attorney and executor of 7 estates

was indicted on Federal charges after he allegedly defrauded the estates of approximately \$1,666,671 by withdrawing cash from the estate accounts without authorization and using the money for personal expenses while mischaracterizing the withdrawals as estate expenses from November 2008 – February 2015. The executor also allegedly laundered fraud proceeds by using funds from one estate to conceal the depletion of the funds from another estate in July 2014.

Source: <https://www.justice.gov/usao-wdky/pr/louisville-attorney-charged-wire-fraud-and-money-laundering>

For additional stories, see items [25](#) and [28](#)

Transportation Systems Sector

9. *March 10, Albany Democrat-Herald* – (Oregon) **One injured in crash, all lanes of Highway 34 now open.** Westbound lanes of Interstate 34 in Corvallis were closed for more than 3 hours March 9 following a two-vehicle crash involving a semi-truck and another vehicle that sent one person to the hospital.
Source: http://www.gazettetimes.com/albany/news/local/one-injured-in-crash-all-lanes-of-highway-now-open/article_fd0a22be-4e56-5990-b11f-444c4e3b1a10.html
10. *March 9, Washington Post* – (Virginia) **Injured are in stable condition after bus collides with truck in Lorton.** A 2-vehicle crash involving a Greyhound bus and another vehicle left 12 people injured March 9 and shut down 3 westbound lanes of Route 123 in Lorton for approximately 3 hours.
Source: <https://www.washingtonpost.com/news/dr-gridlock/wp/2016/03/09/part-of-route-123-in-lorton-is-closed-after-a-bus-collides-with-a-truck>

For another story, see item [30](#)

Food and Agriculture Sector

11. *March 10, U.S. Environmental Protection Agency* – (International) **Mansfield, Mass. pesticide company pays penalty for reporting failures.** The U.S. Environmental Protection Agency (EPA) announced March 9 that Rolf C. Hagen Corp., agreed to pay \$151,040 to settle claims that it imported regulated pesticidal devices to its Mansfield, Massachusetts facility in violation of the Federal Insecticide, Fungicide, and Rodenticide Act after the company failed to submit the required documents to the EPA before importing the devices designed to destroy algae and filter ponds and fish tanks from 2010 – 2014.
Source:
<http://yosemite.epa.gov/opa/admpress.nsf/0/d68c9152079af04a85257f71006edd7f>
12. *March 9, U.S. Food and Drug Administration* – (Oregon) **Eatin' Alive issues allergy alert on undeclared soy in Thai Peanut Noodles and Thai Wrap.** Eatin' Alive issued a recall March 7 for its Thai Peanut Noodles products sold in 8-ounce packages and its Thai Wrap products sold in 6-ounce packages due to an undeclared presence of soy allergens in products containing Tamari. No allergic reactions have been reported

and the products were distributed via direct delivery in the Portland metro area.

Source: <http://www.fda.gov/Safety/Recalls/ucm489949.htm>

13. *March 9, U.S. Food and Drug Administration* – (International) **Wonderful Pistachios voluntarily recalls pistachios due to possible health risk.** The Wonderful Company LLC issued a voluntary recall March 9 for a limited number of flavors and sizes of its in-shell and shelled pistachio products sold in 23 variations after the U.S. Centers for Disease Control and Prevention reported that some of the products may be linked to an outbreak of Salmonellosis. The products were distributed to retail locations nationwide and Canada.

Source: <http://www.fda.gov/Safety/Recalls/ucm489959.htm>

14. *March 9, USA Today* – (International) **Select packages of Corona beer being recalled.** Constellation Brands, Inc.'s Beer Division issued a voluntary recall March 9 for select packages of its Corona Extra products sold in 12-ounce bottles as part of 12-pack and 18-pack packages after routine inspections at 2 of the company's manufacturers revealed that the bottles may contain small pieces of glass. No injuries have been reported in connection to the recall which affects bottles with deposit labels in the U.S. and Guam.

Source: <http://www.usatoday.com/story/money/2016/03/09/select-packages-corona-being-recalled/81544608/>

Water and Wastewater Systems Sector

15. *March 10, Associated Press* – (Ohio) **5,000 gallons of waste water spills into Belmont Co. reservoir.** Approximately 5,000 gallons of waste water spilled into a Belmont County, Ohio reservoir March 9 after a semi-truck overturned and spilled its load. The driver of the semi-truck was taken to the hospital with non-life-threatening injuries and officials believe it will take several days for crews to clean up the spill.

Source: <http://wkbn.com/2016/03/10/5000-gallons-of-waste-water-spills-into-belmont-co-reservoir/>

16. *March 10, Manhattan International Business Times* – (California) **Westlands water district, nation's largest agricultural water district, hit with rare federal fine.** The U.S. Securities and Exchange Commission (SEC) announced March 9 that the Westlands Water District in central California agreed to pay \$125,000 to settle allegations that the district misled investors into believing that it had enough revenue to cover debt payments without having to raise rates and overstated the agency's revenue in order to promote investment in a \$77 million bond issue in 2012. In addition, the district's general manager and the former assistant to the general manager agreed to pay a total of \$70,000 to settle charges that the duo left investors unaware of the Westlands Water District's financial condition.

Source: <http://www.ibtimes.com/westlands-water-district-nations-largest-agricultural-water-district-hit-rare-federal-2333733>

For another story, see item [2](#)

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

17. *March 9, WISN 12 Milwaukee* – (Wisconsin) **West Allis Central classes canceled Wednesday, Thursday after threats.** Classes at West Allis Central High School in Wisconsin were cancelled March 10 following a series of bomb threats that prompted classroom interruptions and evacuations beginning March 7. Police are offering a reward for information on the threats and continue to investigate.
Source: <http://www.wisn.com/news/west-allis-central-high-school-evacuated/38422532>
18. *March 9, WITI 6 Milwaukee* – (Wisconsin) **Data breach impacting Ozaukee Co. employees didn't happen internally, locally.** Ozaukee County officials notified approximately 200 county employees March 8 of a February 14 data breach affecting the county's payroll and tax portal software Greenshades after numerous logins from suspicious Internet Protocol (IP) addresses were found, allowing hackers to view employees W-2 and 1095C tax forms. The county is investigating and became aware of the theft after several employees received notice of suspected fraud from the U.S. Internal Revenue Service.
Source: <http://fox6now.com/2016/03/09/latest-data-breach-impacting-ozaukee-co-employees-didnt-happen-internally-locally/>
19. *March 9, KDKA 2 Pittsburgh* – (Pennsylvania) **Ex-VFW commander accused of racking up thousands in debt on organization credit card.** The former Beaver County Veterans of Foreign Wars commander was charged March 9 with allegedly charging over \$103,000 for personal expenses on the organization's credit card between October 2012 and April 2014.
Source: <http://pittsburgh.cbslocal.com/2016/03/09/ex-vfw-commander-accused-of-racking-up-thousands-in-debt-on-organization-credit-card/>
20. *March 9, CNN* – (New Jersey) **Elevated levels of lead found in water at Newark schools.** The mayor of Newark announced March 9 that 30 Newark Public Schools shut off drinking fountains and posted signs after testing showed elevated levels of lead in the water. Officials stated that alternative water sources would be provided.
Source: <http://www.cnn.com/2016/03/09/us/newark-schools-lead-levels-water/index.html>

For another story, see item [30](#)

Emergency Services Sector

21. *March 10, Associated Press* – (Iowa) **Guns stolen from Iowa police department.** The chief of the Mar-Mac Unified Police Department in Iowa announced March 10 that the department is searching for individuals who stole an undisclosed amount of guns between February 8 and February 17 from a Marquette city garage attached to the

police department's building during renovations.

Source: <http://www.kcci.com/news/guns-stolen-from-iowa-police-department/38439858>

Information Technology Sector

22. *March 10, Softpedia* – (International) **600,000 TFTP servers can be abused for reflection DDoS attacks.** Researchers from the Edinburgh Napier University reported that a combination of flaws in Trivial File Transfer Protocol (TFTP) and publicly-exposed TFTP servers can easily be exploited for attackers to abuse misconfigured setups for reflection denial-of-service (DDoS) attacks after finding that 599,600 TFTP servers were publicly open and had an amplification factor of 60. The vulnerable TFTP servers can be used to launch attacks on other Internet-available services, or used as a pathway for targets inside a closed network.
Source: <http://news.softpedia.com/news/600-000-tftp-servers-can-be-abused-for-reflection-ddos-attacks-501568.shtml>
23. *March 10, The Register* – (International) **Cisco patches a bunch of cable modem vulns.** Cisco Systems reported three vulnerable systems were open to attackers including two wireless gateways, the DPC3941 and DPC3939B, that can allow attackers to exploit the Web-based administration interface via specially crafted Hypertext Transfer Protocol (HTTP) requests; two cable modems, the DPC2203 and EPC2203, that can allow attackers to execute remote code execution via an HTTP input validation vulnerability; and one gateway, the DPQ 3925, that can allow attackers to perform denial-of-service (DDoS) attacks via an HTTP handling flaw.
Source:
http://www.theregister.co.uk/2016/03/10/cisco_patches_a_bunch_of_cable_modem_vulns/
24. *March 9, Softpedia* – (International) **Samsung fixes driver update tool to prevent malicious takeover.** Samsung released updates for its SW Update Tool patching two security-related issues that could have been exploited to perform Man-in-the-Middle (MitM) attacks after a security researcher from Core Security discovered that when contacting Samsung's servers, the SW Update Tool sent all users' information in cleartext and did not check for the data's authenticity after the software received the driver downloads from Samsung's servers. Samsung patched the issues by implementing a ciphered communication between the tool and its servers, and inputting a verification mechanism of the downloaded drivers.
Source: <http://news.softpedia.com/news/samsung-fixes-driver-update-tool-to-prevent-malicious-takeover-501547.shtml>
25. *March 9, SecurityWeek* – (International) **Triada trojan most advanced mobile malware yet: Kaspersky.** Security researchers from Kaspersky discovered a new trojan reportedly believed to be the most advanced mobile malware yet, dubbed Triada that targets Android operating system (OS) devices to redirect financial short message service (SMS) transactions to buy additional content or steal money from victims via an advertising botnet that is embedded with rooting capabilities. The trojan also uses the

Zygot parent process to implement its code in the context of all software on the target's device, allowing the trojan to run in each application.

Source: <http://www.securityweek.com/triada-trojan-most-advanced-mobile-malware-yet-kaspersky>

For another story, see item [28](#)

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

26. *March 9, Telecomlead.com* – (Florida) **Net One faces \$1.6 mn penalty for illegal billing.** The U.S. Federal Communications Commission (FCC) imposed a \$1.6 million penalty on Florida-based Net One International March 9 for billing more than 100 consumers for unauthorized charges and fees in an illegal practice known as “cramming.” Officials advised consumers to contact the FCC if they were improperly charged.

Source: <http://www.telecomlead.com/telecom-services/net-one-faces-1-6-mn-penalty-illegal-billing-67878>

Commercial Facilities Sector

27. *March 10, WVIT 30 New Britain* – (Connecticut) **9 injured, 4 critical in West Hartford Apartment Building fire.** Approximately 100 residents were displaced and 9 other were injured March 10 following a fire at the Westwood Apartments that began on the second floor. Fire crews contained the incident and officials reported the fire spread to the entire building as there were no sprinklers in the building.

Source: <http://www.nbcconnecticut.com/news/local/Fire-Breaks-Out-at-West-Hartford-Apartments-371626841.html>

28. *March 9, Softpedia* – (National) **Rosen Hotel Chain had a PoS malware infection for 17 months.** Florida-based Rosen Hotels & Resorts Inc., reported March 9 that its payment processing system was compromised after a security company discovered malware installed in its credit card systems, which allowed attackers to steal customer data including cardholders' names, card numbers, expiration dates, and internal verification codes from September 2014 – February 2016.

Source: <http://news.softpedia.com/news/rosen-hotel-chain-had-a-pos-malware-infection-for-17-months-501530.shtml>

29. *March 9, Florida Times-Union* – (Florida) **Man dead, suspect in custody after shooting at Jacksonville landscape business.** The Jacksonville Sheriff's Office is investigating a March 9 shooting at the B&L Landscaping Co. after an employee

opened fire and killed one employee. The company was closed March 10 and officials reported that the incident was the second shooting in three days at an area workplace. Source: <http://jacksonville.com/news/crime/2016-03-09/story/man-dead-suspect-custody-after-shooting-jacksonville-landscape-business>

For another story, see item [30](#)

Dams Sector

30. *March 10, Associated Press* – (Louisiana) **3,500 homes evacuated in northern Louisiana because of flooding.** Approaching rain storms in Bossier City, Louisiana, prompted the evacuation of 3,500 homes March 10 due to the threat of a bayou approaching the top of its levee, caused the closure of several sections of Interstate 20, prompted a State of emergency in several Louisiana parishes, and forced the closure of Bossier Parish public schools and Northwestern State University campuses. Source: http://www.nola.com/weather/index.ssf/2016/03/bossier_city_home_evacuations.html
31. *March 9, La Crosse Tribune* – (Wisconsin) **Corps of Engineers to reopen Lock and Dam 9 earlier than expected.** The U.S. Army Corps of Engineers announced March 9 that they will be reopening Lock and Dam 9 near Lynxville five days earlier than scheduled after the lock was closed December 2015 due to winter maintenance. Source: http://lacrossetribune.com/corps-of-engineers-to-reopen-lock-and-dam-earlier-than/article_e8dc3ead-8aeb-524f-ac8e-b2babaac888d.html

For another story, see item [15](#)



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.