Daily Open Source Infrastructure Report
22 December 2014

Top Stories

- A Slidell man and a Kenner doctor pleaded guilty in federal court in New Orleans, Louisiana, December 17 to directing a $56 million Medicare fraud scheme between 2007 and 2014. – *Associated Press* (See item **14**)
- The Office of Personnel Management alerted more than 40,000 federal employees nationwide that their personal information may have been exposed following a breach at federal contractor KeyPoint Government Solutions that was confirmed December 18. – *CBS News; Associated Press* (See item **16**)
- A December 19 fire at an under-construction condominium complex in Orem, Utah, caused an estimated $1 million in damage. Officials are investigating the blaze and reported that it appears to have been intentionally set. – *Associated Press* (See item **27**)
- Authorities reported December 18 that an investigation into a December 8 fire at an under-construction apartment complex in downtown Los Angeles found that the blaze was the result of an act of arson with an estimated $30 million in damages. – *Reuters* (See item **29**)

Fast Jump Menu

Energy Sector

1. *December 19, Threatpost* – (National) **Emerson patches series of flaws in controllers used in oil and gas pipelines.** Researchers identified and reported several vulnerabilities in Emerson Process Management's ROC800 remote terminal units (RTU) widely used in oil and gas pipelines and other applications, and has issued patches for all vulnerabilities except for an authentication bypass issue. The company recommends that customers install a secure router in front of the vulnerable products to mitigate this vulnerability.
   Source: http://threatpost.com/emerson-patches-series-of-flaws-in-controllers-used-in-oil-and-gas-pipelines/109985

[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 18, U.S. Department of Labor* – (Ohio) **OSHA investigation finds workers exposed to lead, copper fumes at Republic Metals in Cleveland.** An investigation prompted by a complaint at the Republic Metals Inc. facility in Cleveland found 19 serious safety and health violations, including exposing workers to copper and lead fumes. Proposed fines totaled $42,800.
   Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=27156

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

3. *December 19, Help Net Security* – (International) **New Zeus variant targets users of 150 banks.** Researchers with Kaspersky Lab identified a new variant of the Zeus banking and information-stealing malware known as Chthonic that is targeting customers of 150 banks and 20 payment systems in the U.S. and 14 other countries. Chthonic shares several components with other forms of malware and is delivered by spam emails or though downloader malware already present on victims' computers.
Source: http://www.net-security.org/malware_news.php?id=2934

4. *December 18, U.S. Securities and Exchange Commission* – (International) **SEC charges additional participant in penny stock manipulation ring.** The U.S. Securities and Exchange Commission announced settled charges December 18 against a man in Nevada for setting up fake Panamanian companies and opening brokerage accounts that were used in an $11 million penny stock manipulation scheme involving the stock of now-defunct Rudy Nutrition. Thirteen other individuals were previously charged in the fraud scheme.
Source: http://www.sec.gov/litigation/litreleases/2014/lr23162.htm

5. *December 18, U.S. Securities and Exchange Commission* – (National) **SEC charges Staten Island-based firm with operating boiler room scheme targeting seniors.** The U.S. Securities and Exchange Commission filed charges December 18 against New York-based Premier Links Inc., its former president, and two sales representatives for allegedly operating the firm as a boiler room scheme that defrauded over 300 investors from across the country of at least $9 million. The company and its members allegedly cold-called individuals and used pressure tactics and fraudulent claims and then redirected most investments to entities the defendants controlled.
Source: http://www.sec.gov/news/pressrelease/2014-287.html

6. *December 18, Easton Express-Times* – (Pennsylvania) **Bethlehem Township restaurant used in $160,000 credit card fraud, court records say.** One person was arrested and arrest warrants were issued December 18 for three others, including the former owner of the Valley Family Restaurant, for allegedly using the business to run fraudulent transactions totaling $160,005. One of the defendants also allegedly provided a skimming device to be set up at the restaurant, though it had not yet been used.
Source:
http://www.lehighvalleylive.com/bethlehem/index.ssf/2014/12/bethlehem_township_restaurant.html

7. *December 18, Whittier Daily News* – (California) **Whittier raid nets guns, drugs hundreds of fraudulent credit cards.** Police in Whittier, California, arrested four individuals in a raid December 18 that uncovered hundreds of fraudulent payment cards, card manufacturing equipment, and stolen checks and IDs.
Source: http://www.whittierdailynews.com/general-news/20141218/whittier-raid-nets-guns-drugs-hundreds-of-fraudulent-credit-cards

For another story, see item **25**

[Return to top]

Transportation Systems Sector

8. *December 18, Reuters* – (California) **Most steel fasteners safe on San Francisco-Oakland Bay Bridge: officials.** State investigators released a draft report December 18 addressing the safety of steel rods and bolts used in a new section of the San Francisco-Oakland Bay Bridge stating that they are safe despite cracks that were found in about 32 fasteners in the same area of the bridge that replaced a portion of the bridge following a 1989 earthquake. The report found that the damaged rods and bolts were weakened by sitting in puddles of rainwater for up to 5 years and that the remaining 2,200 connections had not been exposed to similar conditions.
Source: http://www.reuters.com/article/2014/12/18/us-usa-california-bridge-idUSKBN0JW2LJ20141218

9. *December 18, Arizona Republic* – (Arizona) **Phoenix city bus crash injures 6.** The Phoenix Fire Department responded to a crash involving a Valley Metro city bus December 18 that injured six passengers.. The cause of the accident is under investigation. Source:
http://www.azcentral.com/story/news/local/phoenix/2014/12/18/phoenix-city-bus-crash-injures-six/20606305/

[Return to top]

Food and Agriculture Sector

10. *December 19, U.S. Food and Drug Administration* – (National) **Zachary Confections, Inc. announces a nationwide voluntary recall of Market Pantry (Target) Dark Chocolate Covered Almonds for undeclared peanut in product.** The U.S. Food and Drug Administration reported December 18 that Indiana-based Zachary Confections, Inc., issued a recall for one lot of its Market Pantry Dark Chocolate Covered Almonds due to undeclared peanuts. The product was packaged in 9-ounce containers and sold exclusively at Target Stores nationwide.
Source: http://www.fda.gov/Safety/Recalls/ucm427539.htm

11. *December 18, U.S. Department of Labor* – (Ohio) **OSHA cites Basic Grain Products after 2 workers injured at Coldwater, Ohio, rice-cake plant.** The Occupational Safety and Health Administration cited Basic Grain Products Inc., for two repeat and five serious safety violations following an investigation of the Coldwater, Ohio rice-cake manufacturing facility which was initiated in response to a compliant of a worker electrical shock injury. Proposed penalties total $58,410.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=27150

[Return to top]

Water and Wastewater Systems Sector

12. *December 18, Long Beach Press-Telegram* – (California) **Sewage spill forces closure of Alamitos Bay.** The Alamitos Bay was closed to swimmers December 18 after approximately 5,250 gallons of sewage spilled into the bay December 17 when a 12-inch sewer main ruptured spilling around 11,250 gallons of sewage in total. The beach was expected to remain closed until lab results from daily testing confirm that the water is safe for swimming.
Source: http://www.presstelegram.com/general-news/20141218/sewage-spill-forces-closure-of-alamitos-bay

[Return to top]

Healthcare and Public Health Sector

13. *December 19, South Jersey Times* – (New Jersey) **Evesham police: Receptionist stole $129,000 in patient co-pays.** A receptionist at Aesthetic Dermatology in Marlton was charged December 18 to allegedly stealing more than $129,000 in co-pays from patients over a 2-year period as well as theft by deception for submitting fraudulent time cards, resulting in the overpayment of $10,396 in wages.
Source:
http://www.nj.com/south/index.ssf/2014/12/evesham_police_receptionist_stole_129000_in_co-pays_from_patients.html

14. *December 18, Associated Press* – (Louisiana) **Mastermind of Medicare fraud scheme, doctor plead guilty in New Orleans.** A Slidell man and a Kenner doctor pleaded guilty in federal court in New Orleans December 17 to directing a $56 million Medicare fraud scheme between 2007 and 2014. The scheme used multiple companies under their control and paid kickbacks to patient recruiters who provided Medicare beneficiary numbers that were then used to bill Medicare for unnecessary or unperformed procedures.
Source:
http://www.greenfieldreporter.com/view/story/b239991fa96d446194d0fa0fd68ce9c8/LA--Medicare-Fraud

[Return to top]

Government Facilities Sector

15. *December 19, KIRO 7 Seattle* – (Washington) **Middle school closed Friday after threatening note found.** Pacific Cascade Middle School in Issaquah was closed for a third straight day December 19 as a precaution after a threatening letter was found on campus December 17 threating violence against four staff members as well as threats about violence at lunch or during the winter assembly December 19.
Source: http://www.kirotv.com/news/news/middle-school-closed-friday-after-threatening-note/njXBm/

16. *December 18, CBS News; Associated Press* – (National) **Files of more than 40,000 federal workers breached in cyberattack.** The Office of Personnel Management alerted more than 40,000 federal employees nationwide that their personal information may have been exposed following a breach at federal contractor KeyPoint Government Solutions that was confirmed December 18.
Source: http://www.cbsnews.com/news/files-of-more-than-40000-federal-workers-breached-in-cyberattack/

[Return to top]

Emergency Services Sector

17. *December 19, NJ.com* – (New Jersey) **Former N.J. fire department treasure admits he stole $19K to buy beer, diapers.** A former treasure of the Seaville Volunteer Fire and Rescue Company in New Jersey pleaded guilty December 18 to stealing more than $19,000 by using fire company funds to reimburse himself for personal expenses.
Source: http://www.nj.com/cape-may-county/index.ssf/2014/12/former_nj_fire_department_treasurer_admits_stealing_19k.html

18. *December 18, WSAU* – (Wisconsin) **9-1-1 service interrupted by cut fiber optic line.** Emergency 9-1-1 service and high speed internet service was disrupted in parts of Columbia, Juneau, Adams, and Marquette counties December 18 after a Frontier Communications fiber optic line was inadvertently cut by a third party contractor. Crews repaired the severed line and service was restored about 7 hours later.
Source: http://wsau.com/news/articles/2014/dec/19/9-1-1-service-interrupted-by-cut-fiber-optic-line/

[Return to top]

Information Technology Sector

19. *December 19, Help Net Security* – (International) **Critical flaw on over 12M routers allows device hijacking, network compromise.** Check Point researchers identified a vulnerability in over 12 million routers dubbed “Fortune Cookie” caused by an error within the HTTP cookie management component that could be remotely exploited to cause the current session to be given administrative privileges by sending a packet to a user’s public IP address. The vulnerability was found in routers manufactured by TP-Link, Huawei, Zyxel, Netcomm, SmartAX, Edimax, and others.
Source: http://www.net-security.org/secworld.php?id=17776

20. *December 19, Securityweek* – (International) **Privilege escalation vulnerability found in Linux kernel.** A researcher at AMA Capital Management identified a vulnerability in the Linux kernel that could be used to perform a denial of service (DoS) attack. The vulnerability is related to another recent Linux vulnerability (CVE-2014-9090) and is closed by the patch for the previous vulnerability.
Source: http://www.securityweek.com/privilege-escalation-vulnerability-found-linux-

kernel

21. *December 19, Help Net Security* – (International) **Critical Git flaw allows attackers to compromise developers' machines.** GitHub released a patch for a vulnerability found in the Windows and OS X versions of its official Git client that could have allowed attackers to perform arbitrary command execution. Users were advised to apply the patch as soon as possible.
Source: http://www.net-security.org/secworld.php?id=17774

22. *December 18, Softpedia* – (International) **Exploits for Silverlight, Flash Player and Internet Explorer most used in 2014.** Trend Micro released a report which found that most exploit kits analyzed in 2014 targeted four vulnerabilities for Internet Explorer, Flash Player, and Silverlight. The researchers found that most of the exploits were not the most recent but relied on victims not updating their software, among other findings.
Source: http://news.softpedia.com/news/Exploits-for-Silverlight-Flash-and-IE-Most-Used-in-2014-467883.shtml

23. *December 18, Securityweek* – (International) **SAP patches bugs in business apps.** SAP released patches for two vulnerabilities in its BASIS and SAP BusinessObjects enterprise software discovered by researchers with Onapsis. The most serious vulnerability affected SAP BusinessObjects and could have been used to access and modify information stored on the software's server.
Source: http://www.securityweek.com/sap-patches-bugs-business-apps

For additional stories, see items **3** and **25**

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

See item **18**

[Return to top]

Commercial Facilities Sector

24. *December 19, KTVK 3 Phoenix* – (Arizona) **Man stabbed at Phoenix restaurant.** Police are searching for a suspect who allegedly stabbed another individual several times during an altercation inside the Los Armandos fast-food Mexican restaurant in Phoenix December 19.

Source: http://www.azfamily.com/news/local/Man-stabbed-at-Phoenix-restaurant-286344051.html

25. *December 19, Softpedia* – (International) **AutoIt script loads new "Spark" point of sale malware into RAM.** Trustwave researchers found that a recently-discovered point of sale (PoS) RAM scraper malware dubbed Spark has been distributed using AutoIt-compiled script as a loader to deliver the malware victims' systems. Researchers found that Spark appears very similar to the Alina malware.
Source: http://news.softpedia.com/news/AutoIt-Script-Loads-New-Spark-Point-of-Sale-Malware-Into-RAM-467972.shtml

26. *December 19, WABC 7 New York City* – (New York) **5-alarm fire destroys Ozone Park, Queens building; leaves families homeless.** A 5-alarm fire at an apartment building in the Queens area of New York City December 18 displaced about 80 residents from the building's 24 units that were destroyed by the blaze. Authorities are investigating to determine if the fire is connected to a previous report of smoke coming from a breaker box.
Source: http://7online.com/news/5-alarm-fire-destroys-ozone-park-apartment-building/442427/

27. *December 19, Associated Press* – (Utah) **Orem fire caused $1M in damage, could be arson.** A December 19 fire at an under-construction condominium complex in Orem caused an estimated $1 million in damage. Officials are investigating the blaze and reported that it appears to have been intentionally set.
Source: http://www.cachevalleydaily.com/news/state/article_2839081b-d25f-5317-ae8e-5f4d5d47812c.html

28. *December 19, Tallahassee Democrat* – (Florida) **Apartment fire displaces 20, hospitalizes 1.** One person was hospitalized and 20 residents were displaced following a December 19 apartment fire in Tallahassee. The cause of the fire is under investigation.
Source: http://www.tallahassee.com/story/news/local/2014/12/19/apartment-fire-displaces-20-hospitalizes-1/20629719/

29. *December 18, Reuters* – (California) **Massive Los Angeles construction fire was arson, authorities say.** Authorities reported December 18 that an investigation into a December 8 fire at an under-construction apartment complex in downtown Los Angeles found that the blaze was the result of an act of arson. The fire caused up to $30 million in damage as it engulfed an entire city block, damaged nearby buildings, and caused significant road closures in the area.
Source: http://www.reuters.com/article/2014/12/19/us-usa-california-fire-idUSKBN0JX08C20141219

For another story, see item **6**

[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