Daily Open Source Infrastructure Report
15 April 2016

Top Stories

- Four cars on a BNSF Railway train derailed April 13 in Lafayette Parish, Louisiana, prompting the evacuation of 100 – 110 households after a tanker that contained phosphoric acid was knocked off the tracks. – *Baton Rouge Advocate* (See item **4**)

- Bomb threats made via robocalls prompted a search of at least 21 schools in Bergen and Passaic counties April 13. – *Bergen County Record* (See item **9**)

- Google released patches addressing several vulnerabilities in its account recovery process after a researcher named "Ramzes" found that attackers could change a user's password and hijack a user's account by executing arbitrary code in the context of a help article. – *SecurityWeek* (See item **13**)

- White House officials announced April 13 that a new non-partisan commission will help gather input from subject matter experts (SMEs) for the Federal government and the private sector to strengthen cybersecurity awareness, protect privacy, and ensure public safety and economic and national security. – *SecurityWeek* (See item **14**)

Fast Jump Menu

Energy Sector

Nothing to report

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

1. *April 14, KMOV 4 St. Louis* – (Missouri) **Same man may be behind several skimming devices at local ATMs.** Police authorities were searching April 13 for a man suspected of installing multiple skimming devices on ATMs in Glendale, Maryland Heights, Webster Groves, and St. Louis City in Missouri after security camera footage showed the suspect installing and removing a device at a Royal Banks of Missouri in Glendale. Authorities stated the suspect stole credit card information from 6 customer cards and made over $4,000 in fraudulent purchases using the cards. Source: http://www.kmov.com/story/31718770/same-man-may-be-behind-several-skimming-devices-at-local-atms

2. *April 13, Reuters* – (National) **Fund manager falsely promised tech investments, bought Maserati: U.S.** The U.S. District Court for the Southern District of New York charged 2 executives from Florida-based Elm Tree Investment Advisors LLC April 13 for bilking investors out of $17 million from June 2013 – December 2014 as part of a fraudulent technology investment scheme by falsely assuring investors that the pair had close ties to elite venture capital firms and claiming that they would invest the funds in companies like GoDaddy Inc., Twitter Inc., and Uber Technologies Inc., at opportune times. Officials stated that the executives used the investor's funds for personal expenses, repaid previous investors in a Ponzi-like scheme, and lost nearly $4 million through trading. Source: http://www.reuters.com/article/us-usa-crime-elmtree-idUSKCN0XA2FE

Transportation Systems Sector

3. *April 14, WAAY 31 Huntsville* – (Alabama) **ALDOT worker killed in I-65 crash.** An

Alabama Department of Transportation worker was killed and a second worker was injured in a multi-vehicle crash that shutdown Interstate 65 near Hartselle and Priceville for more than 3 hours April 14.
Source: http://www.waaytv.com/appnews/update-traffic-on-i--reopens-after-early-morning-wreck/article_6da249c2-022c-11e6-94a1-b34fe68e2713.html

4. *April 13, Baton Rouge Advocate* – (Louisiana) **More than 100 homes evacuated following train derailment in Scott; evacuation order lifted at 8:15 p.m.** Four cars on a BNSF Railway train derailed April 13 near Pecan Grove and Walker roads in Lafayette Parish, Louisiana, prompting the evacuation of 100 – 110 households, the G&R Mobile Park, and Little Blessings & Preschool II after a tanker that contained phosphoric acid was knocked off the tracks. No injuries were reported and the tanker did not rupture.
Source: http://theadvocate.com/news/15477762-32/train-derailment-in-scott-forces-evacuation-as-hazmat-crews-work-scene

5. *April 13, KPRC 2 Houston* – (Texas) **I-10 Katy Freeway west at Highway 6 reopens after gas leak.** Westbound lanes of Interstate 10 Katy Freeway in Houston were closed for approximately 2 hours April 13 while crews stopped and repaired a gas leak under the freeway.
Source: http://www.click2houston.com/news/gas-leak-shuts-down-katy-freeway

Food and Agriculture Sector

Nothing to report

Water and Wastewater Systems Sector

6. *April 13, Port Huron Times Herald* – (Michigan) **Combined sewer discharges 35,000 gallons of wastewater.** The Port Huron Wastewater Treatment Plant reported April 13 that approximately 33,000 gallons of combined wastewater and 2,000 gallons of sanitary wastewater spilled into the Black River for 5 hours April 10 – April 11 following heavy rainfall.
Source: http://www.thetimesherald.com/story/news/local/community/2016/04/13/combined-sewer-discharges-35000-gallons-wastewater/83002054/

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

7. *April 14, Detroit News* – (Michigan) **Higher lead, copper levels in 19 Detroit schools' water.** District officials announced April 13 initial testing found elevated lead or copper levels at 19 Detroit Public Schools. Drinking fountains were shut off until further notice and additional bottled water was provided while the district awaits final

test results.
Source: http://www.detroitnews.com/story/news/local/detroit-city/2016/04/13/elevated-lead-levels-found-detroit-schools-water/83013420/

8. *April 13, KING 5 Seattle* – (Washington) **Data breach at Olympia School District.** Olympia School District in Washington announced April 13 that the personal information of individuals employed in the district in 2015 was inadvertently released April 12 via a phishing scam that appeared as a request from the superintendent. The email sought employee names, Social Security numbers, addresses, and salary information.
Source: http://www.king5.com/news/local/data-breach-at-olympia-school-district/131182312

9. *April 13, Bergen County Record* – (New Jersey) **At least 21 north Jersey schools receive bomb threats.** Bomb threats made via robocalls prompted a search of at least 21 schools in Bergen and Passaic counties April 13. Police spent several hours searching the campuses for suspicious items before they were deemed safe.
Source: http://www.northjersey.com/news/at-least-21-north-jersey-schools-receive-bomb-threats-1.1543624

10. *April 13, Savannah Morning News* – (Georgia) **Seven students sent to hospital following collision involving Savannah-Chatham County school bus.** Seven students were transported to area hospitals following an accident involving a Savannah-Chatham County school bus that was rear-ended by another vehicle near Bull Street and Thackery April 13.
Source: http://savannahnow.com/news-latest-news/2016-04-13/seven-students-sent-hospital-following-collision-involving-savannah

11. *April 13, KMBC 9 Kansas City* – (Missouri) **Data breach affects hundreds of Rockhurst University employees.** Rockhurst University in Kansas City, Missouri, notified about 1,300 individuals April 13, who were employed at the university in 2015 that criminals gained access to their W-2 forms through a targeted phishing scam, exposing names, salary amounts, Social Security numbers, and mailing addresses.
Source: http://www.kmbc.com/news/data-breach-affects-hundreds-of-rockhurst-university-employees/39009814

Emergency Services Sector

12. *April 13, Columbus Ledger-Enquirer* – (Georgia) **One of two inmates from Meriwether County Jail is recaptured.** One of two inmates who escaped from the Meriwether County Jail in Greenville April 12 was recaptured without incident April 13 at a hotel in Hogansville. The second inmate who escaped remains at large.
Source: http://www.ledger-enquirer.com/news/local/crime/article71522417.html

Information Technology Sector

13. *April 14, SecurityWeek* – (International) **Google patches serious account recovery**

vulnerability. Google released patches addressing several vulnerabilities in its account recovery process after a researcher named "Ramzes" found that attackers could change a user's password and hijack a user's account by executing arbitrary code in the context of a help article by specifying a page, which attackers controlled, in an sanitized Universal Resource Language (URL) parameter that could have been exploited when a user activated the account recovery process on google.com.
Source: http://www.securityweek.com/google-patches-serious-account-recovery-vulnerabilities

14. *April 14, SecurityWeek* – (International) **White House announces commission on enhancing national cybersecurity.** White House officials announced April 13 that a new non-partisan commission, the Commission on Enhancing National Cybersecurity will help gather input from subject matter experts (SMEs) for the Federal government and the private sector to strengthen cybersecurity awareness, to protect privacy, and to ensure public safety and economic and national security, as well as encourage the public to better control their digital security by recommending actionable steps each party can implement. The commission is expected to report its findings to the White House by December 2016.
Source: http://www.securityweek.com/white-house-announces-commission-enhancing-national-cybersecurity

15. *April 13, SecurityWeek* – (International) **SAP patches XSS, DoS vulnerabilities.** SAP released patches for several of its various products including five cross-site scripting (XSS) issues, four denial of service (DoS) vulnerabilities, three missing authorization check flaws, and one remote code execution (RCE) vulnerability, among other patched flaws. Customers were advised to apply new updates to their systems to patch the vulnerabilities and prevent business risks in their SAP systems.
Source: http://www.securityweek.com/sap-patches-xss-dos-vulnerabilities

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

16. *April 14, Houston Chronicle* – (Texas) **One dead, 11 injured in gas leak near UT.** An official from the Austin Fire Department reported April 14 that 1 person was killed, 11 others were injured, and several dozen residents were evacuated from the 21 Pearl Apartments April 13 after hydrogen sulfide leaked from the building located in Austin. Officials were working to ventilate the building before deeming the area safe.

Source: http://www.chron.com/news/houston-texas/article/Reports-1-dead-5-hurt-in-hazmat-incident-near-UT-7246897.php

17. *April 13, South Jersey Times* – (New Jersey) **Daycare center, residents evacuated in Glassboro gas main break.** The Glassboro Child Development Center and 12 surrounding homes were evacuated while 40 residents were told to shelter in place in Glassboro, New Jersey, April 13 after contractors ruptured a 6-inch gas line, causing natural gas to be released into the air. Several area roads were closed for several hours while HAZMAT crews inspected residential areas.
Source: http://www.nj.com/gloucester-county/index.ssf/2016/04/daycare_center_residents_evacuated_in_glassboro_ga.html

For another story, see item **4**

Dams Sector

Nothing to report

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.