Daily Open Source Infrastructure Report
29 April 2016

Top Stories

- A mechanical failure due to heavy rainfall at the South Kansas River pump station in Topeka released approximately 2.4 million gallons of untreated wastewater into the Kansas River April 26. – *Topeka Capital-Journal* (See item **13**)
- Cisco reported that Tuto4PC's OneSoftPerDay application was discovered to install potentially unwanted programs, harvest users' personal information, and considered to be a backdoor for 12 million personal computers. – *SecurityWeek* (See item **23**)
- Lifeboat Networks reported April 27 that its network was compromised, exposing its users' information from the Minecraft Pocket Edition mobile game after a security researcher found over 7 million user credentials were available online. – *SC Magazine* (See item **24**)
- Six researchers discovered they could create fake traffic jams and track the movements of any Waze user by reverse engineering the Waze app communications protocol and creating Sybil attacks to insert thousands of malicious users inside the Waze networks. – *Softpedia* (See item **25**)

Fast Jump Menu

Energy Sector

1. *April 27, Pittsburgh Post-Gazette* – (Pennsylvania) **State investigating quakes near Pa. fracking sites.** The Pennsylvania Department of Environmental Protection announced April 27 that it is investigating the cause of a 1.9 earthquake April 25 in Lawrence County near a Hilcorp Energy Co., doing business as North Beaver NC Development site where the company was hydraulically fracturing two wells in a four-well pad in Mahoning Township. State officials reported that the company stopped fracking operations and demobilized following the incident.
Source: http://powersource.post-gazette.com/powersource/companies/2016/04/27/Pennsylvania-DEP-investigating-quakes-near-Hilcorp-Energy-fracking-shale-well-site-Lawrence-County/stories/201604270180

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

2. *April 27, New York Daily News* – (New York) **Bloods-linked gang members charged with running $414G identity-theft ring.** Officials from the New York County District Attorney's Office announced April 26 that 39 gang members were charged for their roles in a $414,000 identity theft scheme where the group used stolen bank information from the Dark Web to create phony credit cards used to make fraudulent purchases at Barneys and Sacks Fifth Avenue stores and sold the goods to fund personal expenses. Officials stated a subsequent search of the suspects' apartments in Queens and Brooklyn, New York revealed computers and credit card making equipment, among other illicit materials.
Source: http://www.nydailynews.com/new-york/nyc-crime/bloods-linked-gang-members-charged-414g-id-theft-ring-article-1.2615754

Transportation Systems Sector

3. *April 28, KOLO 8 Reno* – (Nevada) **Three-vehicle crash at Lake Tahoe sends one**

person to hospital. Highway 50 near Stateline, Nevada, was closed for several hours April 27 following an accident involving three vehicles that left one person injured.
Source: http://www.kolotv.com/content/news/Three-vehicle-accident-sends-one-person-to-the-hospital-377387671.html

4. *April 27, KATU 2 Portland* – (Oregon) **21-year-old Beaverton man killed in wrong-way crash on Highway 26.** Highway 26 eastbound in Beaverton was closed for several hours April 27 following a head-on collision that left one person dead and three others seriously injured.
Source: http://katu.com/news/local/deadly-head-on-sunset-highway-hwy-26-east-eastbound-closed-past-cornell-murray-detour-accident-crash-wrong-way-driver

5. *April 27, San Francisco Bay City News* – (California) **All lanes of I-580 in Pleasanton reopened after fatal crash.** Westbound lanes of Interstate Highway 580 in Pleasanton were closed for approximately 3 hours April 27 while California Highway Patrol officials investigated a collision involving six vehicles that left one person dead.
Source: http://abc7news.com/traffic/fatal-accident-snarls-wb-i-580-commute-in-pleasanton/1311325/

6. *April 27, WRAL 5 Raleigh* – (North Carolina) **One dead in I-95 tractor-trailer wreck.** Northbound lanes of Interstate 95 in Benson were shut down for about 4 hours April 27 while first responders cleared the scene after a semi-truck was rear-ended by another semi-truck, leaving one driver dead.
Source: http://www.wral.com/official-1-dead-in-i-95-tractor-trailer-wreck/15667400/

For another story, see item **25**

Food and Agriculture Sector

7. *April 28, U.S. Food and Drug Administration* – (California) **Bakery Express of Southern California issues allergy alert on undeclared peanut in 7-Eleven Fresh To Go cookies.** Bakery Express of Southern California issued a recall April 28 for its 7-Eleven Fresh To Go brand Chocolate Chunk Cookies, Oatmeal Raisin Cookies, and Peanut Butter Cookie products due to the presence of undeclared peanuts after a supplier notified the company that three different cookie dough pucks used in producing the cookies were potentially contaminated with peanuts. No illnesses have been reported and the products were sold at 7-Eleven stores throughout southern California.
Source: http://www.fda.gov/Safety/Recalls/ucm498079.htm

8. *April 28, U.S. Food and Drug Administration* – (National) **Southeastern Grocers issues voluntary recall on undeclared peanuts in Bakery Crème Cakes.** Southeastern Grocers LLC issued a voluntary recall April 27 for its Bakery Crème Cakes products sold in 32-ounce packages and its Bakery Sliced Crème Cakes products sold in 14-ounce packages due to misbranding and undeclared peanuts after the supplier notified the company that the products potentially contained peanuts. No illnesses have been reported and the products were distributed to all BI-LO, Harveys

Supermarket, and Winn-Dixie stores in 7 States.
Source: http://www.fda.gov/Safety/Recalls/ucm498086.htm

9. *April 28, U.S. Food and Drug Administration* – (National) **Old Home Kitchens issues allergy alert and voluntary recall on undeclared peanuts in "Old Home Kitchens 14oz Sliced Crème Cake."** Old Home Kitchens issued a voluntary recall April 25 for its Old Home Kitchens Sliced Lemon Crème Cake, Sliced Vanilla Crème Cake, and Sliced Strawberry Swirl Crème Cake products sold in 14-ounce packages due to the presence of undeclared peanuts after the supplier notified the company that an ingredient used in the cake products potentially contained peanut allergens. No illnesses have been reported and the products were distributed to retail stores in 16 States.
Source: http://www.fda.gov/Safety/Recalls/ucm498092.htm

10. *April 27, U.S. Food and Drug Administration* – (National) **Schaffner Distributing Pronutri LLC. issues an allergy alert on undeclared soy lecithin and milk in Re-VITA-lize.** Schaffner Distributing Pronutri LLC issued a recall April 26 for one lot of its Re-VITA-lize Tropical Orange Flavor vitamin products sold in 32-ounce packages due to misbranding and an undeclared presence of soy lecithin and milk allergens after it was discovered that a whey protein ingredient was not listed on the label. No illnesses have been reported and the products were distributed to retail locations via direct delivery to six States.
Source: http://www.fda.gov/Safety/Recalls/ucm498017.htm

11. *April 27, U.S. Department of Justice* – (California) **District court enters permanent injunction against San Francisco rice noodle company and senior officers to stop distribution of adulterated products.** The U.S. Department of Justice announced a permanent injunction April 27 against Kun Wo Food Products Inc., and its co-owners following Federal inspections at the San Francisco-based facility which revealed that the company prepared, processed, manufactured, and distributed its rice noodle products under insanitary conditions, and failed to take necessary precautions to prevent food handlers from contaminating the products with microorganisms or foreign materials, among other sanitation violations after testing revealed the presence of L. mono and L. seeligeri in the firm's production area. The injunction requires the firm to improve its manufacturing processes and receive consent from the U.S. Food and Drug Administration in order to resume production.
Source: https://www.justice.gov/opa/pr/district-court-enters-permanent-injunction-against-san-francisco-rice-noodle-company-and

Water and Wastewater Systems Sector

12. *April 28, Temple Daily Telegram* – (Texas) **Storm causes sewage spill in East Temple.** Severe weather caused both primary and secondary electrical lines to fail at the Doshier Farm Wastewater Treatment Plant in East Temple, Texas, April 27 releasing approximately 125,000 gallons of wastewater on site and into an unnamed tributary to Little Elm Creek. Officials issued a boil water advisory for individuals using private drinking water supply wells within a half mile of the spill site.

Source: http://www.tdtnews.com/news/article_e5df4866-0d00-11e6-8a46-a3e232227de6.html

13. *April 27, Topeka Capital-Journal* – (Kansas) **2.4 million gallons of untreated wastewater released into Kansas River in Topeka after storm, mechanical failure.** A mechanical failure due to heavy rainfall at the South Kansas River pump station in Topeka released approximately 2.4 million gallons of untreated wastewater into the Kansas River April 26.
Source: http://cjonline.com/news/2016-04-27/24-million-gallons-untreated-wastewater-released-kansas-river-after-storm-mechanical#

14. *April 27, KNSD 39 San Diego* – (California) **Sewage spill closes lake.** Officials issued a water contact closure for Lake San Marcos in San Marcos, California, after a sewer line broke April 26 spilling about 60,000 gallons of sewage into the lake. The damaged line was expected to be repaired by April 27.
Source: http://www.nbcsandiego.com/news/local/sewage-spill-lake-san-marcos-san-diego-377321591.html

For another story, see item **15**

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

15. *April 28, Hillsboro Reporter* – (Texas) **Lake Whitney Parks close due to flooding.** Officials announced April 28 that due to high lake levels all U.S. Army Corps of Engineers parks on Lake Whitney and Lake Whitney State Park in Texas were closed until further notice.
Source: http://hillsbororeporter.com/lake-whitney-parks-close-due-to-flooding-p20253-54.htm

16. *April 28, Chicago Tribune* – (Illinois) **Chicago to start testing water in some schools for toxic lead.** The mayor of Chicago announced April 27 that Chicago Public Schools will begin initial tests for lead in water at 28 schools in order to help safeguard children. The results will be posted online and city officials will be given guidance as testing is expanded to include other schools.
Source: http://www.chicagotribune.com/news/local/breaking/ct-cps-lead-water-emanuel-met-20160427-story.html

17. *April 28, Middletown Times Herald-Record* – (New York) **Wildfire at Sam's Point 60% under control, mop-up continues.** Crews reached 60 percent containment April 28 of the 1,897-acre wildfire burning in Sam's Point in New York. Authorities stated that the fire is still active and firefighters were focusing on remaining hot spots.
Source: http://www.recordonline.com/article/20160427/NEWS/160429413

18. *April 27, KMGH 7 Denver* – (Colorado) **Student hospitalized after explosion in science room at Hidden Lake High School in Westminster.** Students were evacuated and classes were cancelled at Hidden Lake High School in Westminster April 27 after a student was injured following a chemical reaction in a laboratory class. The building was ventilated and classes were expected to resume April 28.
Source: http://www.thedenverchannel.com/news/front-range/westminster/student-hospitalized-after-explosion-in-science-room-at-hidden-lake-high-school-in-westminster

19. *April 27, Waynesboro News Virginia* – (Virginia) **90 percent of Shenandoah National Park fire contained.** Fire crews reached 90 percent containment April 27 of the 10,326-acre fire burning in the Shenandoah National Park in Virginia.
Source: http://www.dailyprogress.com/news/local/percent-of-shenandoah-national-park-fire-contained/article_dd4b86a7-5bf6-56f4-bb16-8905bdcdeaf4.html

20. *April 27, WJBK 2 Detroit* – (Michigan) **Water main break in Canton closes 2 schools.** ITT Technical Institute Canton and Crescent Academy International in Michigan were closed April 27 due to a water main break. Utility crews reported to the scene to repair the break.
Source: http://www.fox2detroit.com/news/local-news/133366418-story

Emergency Services Sector

Nothing to report

Information Technology Sector

21. *April 28, SecurityWeek* – (International) **Critical, high severity flaws patched in Firefox.** Mozilla released its web browser, Firefox 46 that patched a total of 14 vulnerabilities including 4 critical vulnerabilities affecting the browser engine, which could cause crashes and potential arbitrary code execution, as well as a high severity vulnerability that could be exploited via specially crafted Web content and cause an exploitable crash, among other flaws.
Source: http://www.securityweek.com/critical-high-severity-flaws-patched-firefox

22. *April 28, The Register* – (International) **Time for a patch: Six vulns fixed in NTP daemon.** Security researchers from Cisco's Talos Security Intelligence and Researcher Group discovered five vulnerabilities in Network Time Protocol daemon (ntpd) after its ongoing ntpd evaluation revealed attackers could craft User Datagram Protocol (UDP) packets to cause a denial-of-service (DoS) condition or prevent the correct time from being set, among other actions. The vulnerabilities were patched in Network Time Protocol (NTP) version 4.2.8p7.
Source:
http://www.theregister.co.uk/2016/04/28/time_for_a_patch_six_vulns_fixed_in_ntp_daemon/

23. *April 28, SecurityWeek* – (International) **Cisco finds backdoor installed on 12 million**

PCs. Cisco's Talos Security Intelligence and Research Group reported that a Tuto4PC's OneSoftPerDay application was discovered to install potentially unwanted programs (PUPs), harvest users' personal information, and was considered to be a backdoor for 12 million personal computers (PCs) after an analysis revealed that an increase in generic trojans were found when about 7,00 unique samples displayed names including "Wizz" in some of the domains.
Source: http://www.securityweek.com/cisco-finds-backdoor-installed-12-million-pcs

24. *April 27, SC Magazine* – (International) **Over 7M Minecraft mobile credentials exposed after Lifeboat data breach.** Lifeboat Networks reported April 27 that its network was compromised in January, exposing its users' login names, passwords, and email addresses in the Minecraft Pocket Edition mobile game after a security researcher found over 7 million user credentials were available online. Lifeboat forced its customers to reset their passwords discretely and stated they started using stronger algorithms to guard user data.
Source: http://www.scmagazine.com/over-7m-minecraft-mobile-credentials-exposed-after-lifeboat-data-breach/article/492634/

25. *April 27, Softpedia* – (International) **Waze drivers can be tracked, network flooded with fake traffic.** Six researchers from the University of California, University of Santa Barbara, and the Tsinghua University discovered that they could create fake traffic jams and track the movements of any Waze user by reverse engineering the Waze app communications protocol and creating Sybil attacks to insert thousands of malicious users inside the Waze networks. The attacks could manipulate the app's behavior and allow attackers to pose as Waze users when communicating with the app's Google server.
Source: http://news.softpedia.com/news/waze-drivers-can-be-tracked-network-flooded-with-fake-traffic-503473.shtml

26. *April 27, SecurityWeek* – (International) **Attackers increasingly abuse open source security tools.** Security researchers from Kaspersky Lab reported that the open source security tool, Browser Exploitation Framework (BeEF) was being leveraged by an advanced persistent threat (APT) group named NewsBeef to track and steal users' browsing history from compromised Web sites through flaws in content management systems. In addition, researchers reported that other APT actors were using open source tools in their operations to execute malware across the globe.
Source: http://www.securityweek.com/attackers-increasingly-abuse-open-source-security-tools

27. *April 27, SecurityWeek* – (International) **Verizon 2016 DBIR: What you need to know.** Verizon released its 2016 Data Breach Investigations Report (DBIR) which revealed current information technology (IT) trends and the overall cyberattack landscape after conducting an analysis on over 100,000 security incidents, which confirmed 2,260 data breaches occurred across 82 different countries in 2015, with the majority of breaches occurring due to human nature via phishing campaigns.
Source: http://www.securityweek.com/verizon-2016-dbir-what-you-need-know

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

See items **24** and **25**

Commercial Facilities Sector

28. *April 28, KPRC 2 Houston* – (Texas) **Lack of hydrants made massive apartment fire hard to fight, firefighters say.** A 3-alarm fire April 27 at the Providence at Champions Apartments in northwest Harris County damaged 16 apartment units and injured 1 person as the apartment complex did not have fire hydrants. Officials were investigating the cause of the blaze.
Source: http://www.click2houston.com/news/hfd-responding-to-massive-apartment-fire-in-northwest-houston

29. *April 27, WPRI 12 Providence* – (Massachusetts) **36 displaced after fire at Fall River apartment complex.** The Fall River Fire Captain reported April 27 that an unattended cooking fire at a Massachusetts apartment complex displaced 36 residents and damaged 3 apartment units. No injuries were reported.
Source: http://wpri.com/2016/04/27/crews-respond-to-fire-at-fall-river-apartment-complex/

For another story, see item **2**

Dams Sector

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