Daily Open Source Infrastructure Report
19 May 2016

Top Stories

- General Motors issued a recall May 17 for 317,572 of its Chevrolet Sonic, Trax, and Spark vehicles equipped with a Bring Your Own Media (BYOM) radio due to a software glitch. – *TheCarConnection.com* (See item **4**)
- A Minnesota man pleaded guilty May 17 to running a $250 million Ponzi scheme across 7 States where he used his business, Minnesota Print Services Inc., to defraud investors by promising stakeholders discounts with major printing corporations if they paid him in cash. – *Southern California City News Service* (See item **6**)
- Metro-North service resumed on an abbreviated schedule May 18 following a May 17 fire that began beneath elevated tracks near Manhattan's East Harlem station, which halted service and left thousands of commuters stranded. – *Associated Press* (See item **10**)
- A senior security researcher at enSilo reported that the malware, Furtim was seen evading antivirus detection due to the malware's ability to search an infected machine for registry entries or service executable names of 400 security products. – *SecurityWeek* (See item **21**)

Fast Jump Menu

Energy Sector

1. *May 17, Associated Press* – (California) **Pipeline company indicted in Refugio oil spill.** The California attorney general announced May 17 that Texas-based Plains All American Pipeline and one if its employees face several criminal charges and up to $2.8 million in penalties following a May 2015 incident where more than 140,000 gallons of crude oil was released from the company's pipeline on to Refugio Beach and into the ocean, harming hundreds of species and marine life. The incident was prompted by a severely corroded underground pipeline that broke on land.
Source: http://abc7.com/news/pipeline-company-indicted-in-refugio-oil-spill/1342313/

Chemical Industry Sector

2. *May 17, Associated Press* – (New Hampshire) **Potentially cancer-causing chemical found in former landfill.** Federal regulators are investigating a chemical leak after the New Hampshire Department of Environmental Services reported May 17 that the potentially cancer-causing chemical, perfluorooctanoic acid (PFOA) was discovered in 50 wells in towns surrounding the Saint-Gobain Performance Plastics facility in Merrimack, as well as in 11 private wells near a former manufacturing site operated by Textiles Coated International in Amherst. In addition, the U.S. Environmental Protection Agency tested monitor wells near the Merrimack landfill and found PFOA levels were five times higher than the Federal limit.
Source: http://www.thestate.com/news/business/national-business/article78111417.html

Nuclear Reactors, Materials, and Waste Sector

3. *May 17, NuclearStreet.com* – (Pennsylvania) **Susquehanna's Unit 2 back on line after four-day shutdown.** Talen Energy officials reported May 17 that its Susquehanna Steam Electric Station Unit 2 nuclear reactor in Salem Township, Pennsylvania, was back online following a four-day manual shutdown due to an issue in one of the unit's 480-volt electrical distribution centers May 13.
Source:
https://nuclearstreet.com/nuclear_power_industry_news/b/nuclear_power_news/archive/2016/05/17/susquehanna_2700_s-unit-2-back-on-line-after-four_2d00_day-shutdown-051701#.VzxkoJErKUk

Critical Manufacturing Sector

4. *May 17, TheCarConnection.com* – (National) **2013 – 2016 Chevrolet Sonic, Trax, 2013 – 2015 Chevrolet Spark recalled for software glitch.** General Motors issued a recall May 17 for 317,572 of its model years 2013 – 2016 Chevrolet Sonic and Trax vehicles, and its model years 2013 – 2015 Chevrolet Spark vehicles equipped with a Bring Your Own Media (BYOM) radio sold in the U.S. due to a software glitch that prevents the radio from providing an audible warning when the driver waits 10 or more minutes to exit the vehicle after turning off the ignition and leaving the key in the cylinder, which can cause the driver to forget the key in the ignition, thereby making

the vehicles more susceptible to theft.
Source: http://www.thecarconnection.com/news/1103991_2013-2016-chevrolet-sonic-trax-2013-2015-chevrolet-spark-recalled-for-software-glitch

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *May 17, WNCT 9 Greenville* – (North Carolina) **Fraud alert: Card skimmers discovered at 4 Greenville First Citizens Bank ATM locations.** Authorities are searching May 17 for the persons responsible for installing card skimmers at four different First Citizen Bank ATM locations in Greenville, North Carolina, after a bank employee discovered one of the malicious card readers during an ATM inspection. Police and First Citizen Bank staff were monitoring account activity for suspicious transactions.
Source: http://wnct.com/2016/05/17/fraud-alert-card-skimmers-discovered-at-4-greenville-first-citizens-bank-atm-locations/

6. *May 17, Southern California City News Service* – (National) **Guilty plea in multi-million-dollar Ponzi scheme.** A Minnesota resident pleaded guilty May 17 to running a $250 million Ponzi scheme where the man used his business, Minnesota Print Services Inc., to defraud investors by claiming he had printing contracts with major corporations and needed cash upfront to receive discounts on purchasing paper, causing investors in 7 States up to $54 million in losses. Officials stated the man used the investors' funds for personal expenses.
Source: http://www.nbclosangeles.com/news/local/Guilty-Plea-in-Multi-Million-Dollar-Ponzi-Scheme-379846151.html

7. *May 17, WJW 8 Cleveland* – (Ohio) **'BDL' bandit robs Warrensville Heights bank.** FBI authorities are searching for a man dubbed the "BDL Bandit" who is suspected of robbing five banks including the First Merit Bank in Warrensville Heights, Ohio, May 17. Authorities stated the suspect is considered armed and dangerous.
Source: http://fox8.com/2016/05/17/bdl-bandit-robs-warrensville-heights-bank/

8. *May 16, KMSP 9 Minneapolis* – (International) **Minnesota woman pleads guilty to faking husband's death for insurance money.** A Minnesota woman pleaded guilty May 16 to defrauding Mutual of Omaha Insurance Company out of more than $2 million in life insurance proceeds by falsely claiming her ex-husband's death after she identified the remains of a body in Moldova as her former husband. Officials stated the woman recruited a third party to open a U.S. bank account and transfered $1.5 million of the insurance proceeds to her son's account, which was then transferred to bank accounts in Switzerland and Moldova from March 2012 – January 2015.
Source: http://www.fox9.com/news/142050073-story

Transportation Systems Sector

9. *May 18, Eau Claire Leader-Telegram* – (Wisconsin) **Highway 35 crash causes fuel spill.** Highway 35 between Buffalo and Pepin counties was closed for nearly 5 hours May 16 after a semi-trailer struck a guardrail and overturned on a bridge, spilling approximately 180 gallons of diesel fuel and oil on the road and into the water below.
Source: http://www.leadertelegram.com/News/Local/Briefs/2016/05/18/Highway-35-crash-causes-fuel-spill-nbsp.html

10. *May 18, Associated Press* – (New York) **After fire, NYC rail passengers endure overcrowded commutes.** Metro-North service resumed on an abbreviated schedule May 18 following a May 17 fire that began at a garden center underneath tracks near Manhattan's East Harlem station, which halted service and left thousands of commuters stranded. More than 150 firefighters responded to the blaze that damaged a column located beneath elevated tracks and involved construction debris.
Source: http://www.miamiherald.com/news/business/article78264692.html

11. *May 18, Associated Press* – (Arizona) **2 dead after small plane crashes near airfield in Arizona.** The U.S. Federal Aviation Administration and the U.S. National Transportation Safety Board are investigating after a single-engine AT-6 plane crashed and exploded near Falcon Field Airport in Phoenix May 17, leaving two people dead.
Source: http://www.msn.com/en-us/news/us/2-dead-after-small-plane-crashes-near-airfield-in-arizona/ar-BBtbmkU?li=BBnb7Kz

For another story, see item **1**

Food and Agriculture Sector

12. *May 17, Food Safety News* – (Minnesota; Virginia) **Officials confirm outbreak linked to Taylor Farms.** The U.S. Centers for Disease Control and Prevention confirmed May 17 that Taylor Farms Organic Kale Medley Power Greens products were responsible for the Salmonella Enteritidis outbreak that sickened six people in Minnesota and one in Virginia since April. The products were sold at Sam's Club locations nationwide and Federal officials are monitoring the outbreak for additional victims.
Source: http://www.foodsafetynews.com/2016/05/officials-confirm-salmonella-outbreak-linked-to-taylor-farms/#.VzsogfkrKUk

Water and Wastewater Systems Sector

13. *May 18, WRBL 3 Columbus* – (Georgia) **Major leak at Columbus water treatment plant.** Columbus Water Works isolated a major water leak at the North Columbus Water Sources Facility on River Road in Georgia that caused reduced service or loss of service for residents for approximately 5 hours May 17. Officials stated that residents may see discolored water for up to 24 hours while the system stabilizes.
Source: http://wrbl.com/2016/05/17/major-leak-at-columbus-water-treatment-plant/

Healthcare and Public Health Sector

14. *May 16, WANE 15 Fort Wayne* – (Indiana) **Hackers hold DeKalb Health computer systems hostage.** DeKalb Health in Indiana announced May 16 that its administrative computers were infected with ransomware, temporarily disrupting operations while officials worked to transfer patients and bring the systems back online. The incident remains under investigation.
Source: http://wane.com/2016/05/16/dekalb-health-hit-with-ransomware/

Government Facilities Sector

15. *May 18, WNBC 4 New York City* – (New York) **Suburban NYC school shuts off drinking water due to lead.** George M. Davis Jr. Elementary School in New York City announced May 16 that it shut off its drinking water sources after testing in March revealed high levels of lead in some of the school's water sources. Officials reported that bottled water and coolers will be provided.
Source: http://www.nbcnewyork.com/news/local/Suburban-NYC-School-Shuts-Off-Drinking-Water-Due-to-Lead--379920291.html

16. *May 17, WAVY 10 Portsmouth* – (Virginia) **17 injured in school bus accident returning from field trip.** Fifteen Ingleside Elementary School students and two adults were transported to an area hospital with injuries after a Norfolk City Public School's bus ran off of Indian River Road and into a ditch in Virginia Beach May 17.
Source: http://wavy.com/2016/05/17/norfolk-school-bus-crashes-in-va-beach-minor-injuries-reported/

17. *May 17, Arizona Republic* – (Arizona) **Officials: Gilbert Public Schools email hacked by junior high school student.** Officials at Gilbert Public Schools in Arizona announced May 17 that a Highland Junior High student gained access to a teacher's login information and emailed inappropriate images to other students. The technology department disabled both accounts and equipped all computers with content filtering and monitoring solutions.
Source: http://www.azcentral.com/story/news/local/gilbert/2016/05/17/gilbert-public-schools-emails-hacked-by-student/84484620/

18. *May 17, Baltimore Sun* – (Maryland) **Maryland fines Baltimore $40,000 for discharging grease, pollutants from wastewater treatment plants.** The Maryland Department of the Environment fined Baltimore City $40,000 May 17 for several permit violations including the discharge of grease and phosphorus from the Patapsco Wastewater Treatment Plant into the harbor on at least a dozen occasions between 2010 and 2013. The city's Board of Estimates will vote May 18 on a consent agreement settling the violations, which could include additional fines for failing to fix problems.
Source: http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-wastewater-plant-fines-20160517-story.html

19. *May 17, Newton Wicked Local* – (Massachusetts) **Test detects high lead levels in water at Newton's Burr Elementary School.** Water service to drinking fountains at

Burr Elementary School in Newton was shut off May 17 after testing revealed high levels of lead in one of the fountains. School officials are providing bottled water until the cause of the lead contamination is determined.
Source: http://newton.wickedlocal.com/article/20160517/NEWS/160516243

Emergency Services Sector

Nothing to report

Information Technology Sector

20. *May 18, SC Magazine* – (International) **Cisco patch blocks DoS vulnerability.** Cisco released patches for its Adaptive Security Appliance (ASA) software after security researchers found attackers could alter a memory block, allowing the system to cease transferring traffic and cause a denial-of-service (DoS) situation. The flaw was reportedly linked to an issue in the installation of Internet Control Message Protocol (ICMP) error handling for Internet Protocol Security (IPSec) packets.
Source: http://www.scmagazine.com/cisco-patch-blocks-dos-vulnerability/article/497148/

21. *May 18, SecurityWeek* – (International) **Windows malware tries to avoid 400 security products.** A senior security researcher at enSilo reported that the malware, Furtim was seen avoiding security detection as the malware has the ability to search the infected machine for registry entries or service executable names of 400 security products, including rare security products, virtualization environments, and sandboxing products. Once the malware detects a security product, the malware terminates itself and leaves the computer unharmed, avoiding any type of detection.
Source: http://www.securityweek.com/windows-malware-tries-avoid-400-security-products

22. *May 17, Softpedia* – (International) **Researcher wins $5,000 for finding XSS bug on Google in most peculiar manner.** A security researcher from ERNW found a "sleeping stored" cross-site scripting (XSS) vulnerability in Google's Cloud Console product which could allow an attacker to create a project with a payload in its name and leave it on the dashboard, tricking an administrator into deleting the unknown project and triggering the exploit. Google was made aware of the exploit.
Source: http://news.softpedia.com/news/researcher-wins-5-000-for-finding-xss-bug-on-google-in-most-peculiar-manner-504174.shtml

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

23. *May 18, Associated Press* – (Florida) **SeaWorld staffer accused of stealing $116K.** A former SeaWorld supervisor was charged May 14 with grand theft and scheme to defraud after she allegedly stole $116,000 from the company's Aquatica water park in Orlando by pocketing money from cash drawers while other employees were on break and voiding ticket sales to steal the funds while working in the guest relations department from 2013 – 2015.
Source: http://www.nbcchicago.com/news/national-international/Affidavit-SeaWorld-Staffer-Voids-Tickets-Pockets-116000-379879811.html

24. *May 18, KCBS 2 Los Angeles* – (California) **3 injured in senior living apartment complex fire in Anaheim.** A 3-alarm fire May 17 at an Anaheim apartment building caused about $400,000 in damages, displaced several residents, and left several apartment units without power due to a grease fire that began in a unit kitchen.
Source: http://losangeles.cbslocal.com/2016/05/18/anaheim-third-alarm-fire-injuries/

25. *May 17, Jersey Journal* – (New Jersey) **Nearly 40 people displaced, 3 injured after 'horrible' Jersey City fire.** A 3-alarm fire at a Jersey City apartment building displaced at least 37 people, injured 3 people, and heavily damaged the facility May 16 after the blaze allegedly began when mattresses in the alleyway caught fire. The incident was contained and the American Red Cross is assisting the displaced residents.
Source:
http://www.nj.com/hudson/index.ssf/2016/05/nearly_40_people_displaced_3_injured_after_horribl.html

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