Daily Open Source Infrastructure Report
18 July 2016

Top Stories

- Three locomotives and 10 rail cars on a Norfolk Southern train derailed July 14 after the train collided with a truck in Wauhatchie Pike in Tennessee, injuring 3 people, and spilling thousands of gallons of diesel fuel. – *Chattanooga Times Free Press* (See item 7)
- Philips advised Xper Connect users to update their operating system (OS) to Microsoft Windows 2008-R2 and install Xper version 1.5 service pack 13 after researchers discovered 460 vulnerabilities in Philips Xper Information Management Connect. – *SecurityWeek* (See item 19)
- Researchers found a new trojan dubbed "Delilah" that uses social engineering and extortion to recruit insiders by collecting personal information in order to blackmail the targeted individual. – *SecurityWeek* (See item 22)
- The Bay State Restorations warehouse in Brockton sustained significant damage July 14 following a seven-alarm fire that forced a nearby Massachusetts Bay Transportation Authority (MBTA) commuter rail station to close. – *Brockton Enterprise* (See item 27)

Fast Jump Menu

Energy Sector

1. *July 15, KOTV 6 Tulsa* – (Oklahoma) **PSO works to restore power across Tulsa metro area.** Public Service Company of Oklahoma crews worked July 15 to restore power to about 38,000 customers who remained without service after storms moved across eastern Oklahoma July 14 knocking out power to more than 100,000 customers. The power outage prompted the closure of summer classes at two schools in the Tulsa Public Schools district.
   Source: http://www.newson6.com/story/32452435/pso-power-may-out-for-some-green-country-customers-for-days

2. *July 15, KOLR 10 Springfield* – (Arkansas) **Thousands without power across Arkansas after storms.** Utility crews worked July 15 to restore power to 90,000 customers who remained without service after severe storms moved through Arkansas July 14 knocking out power to 137,000 customers.
   Source: http://www.ozarksfirst.com/news/thousands-without-power-across-arkansas-after-storms

Chemical Industry Sector

See item **10**

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

3. *July 14, U.S. Department of Labor* – (New Jersey) **Newark metal treatment company faces $87K penalty for exposing workers to fall, chemical, electrical, and compressed gas hazards.** The Occupational Safety and Health Administration cited Bennett Heat Treating and Brazing Co. Inc., with 29 serious and 1 other-than-serious safety and health violations July 8 after January and February 2016 inspections at the Newark, New Jersey facility revealed that the company exposed workers to fall hazards, failed to properly store compressed gases, and used corrosive chemicals without a proper decontamination shower, among other violations. Proposed penalties total $87,500.
   Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=32808

4. *July 14, U.S. Department of Labor* – (Ohio) **OSHA finds lack of machine safety guarding after worker suffers fracture of three fingers at Ohio metal alloy manufacturer.** The Occupational Safety and Health Administration cited Materion Brush Inc., with one willful safety violation July 13 after a March 2016 incident where a worker's fingers were fractured while operating a metal coiler, prompting an inspection at the Elmore, Ohio facility which revealed that the company failed to

ensure the machinery had adequate safety guards installed. Proposed penalties total $70,000.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=32811

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *July 14, WXIX 19 Newport* – (Ohio) **Investigators: Link between skimmers and 103 credit cards found possible.** A New York resident was arrested in Symmes Township, Ohio, July 14 after police found over 103 fraudulent Visa gift cards that had been re-encoded with stolen credit card numbers in the suspect's vehicle during a routine traffic stop. Authorities are investigating whether the man is linked to a credit card skimming scheme targeting New York, New Jersey, and Connecticut.
Source: http://www.fox19.com/story/32448447/investigators-link-between-skimmers-and-103-stolen-credit-cards-found-possible

6. *July 14, Southern California City News Service* – (California) **'Hipster Bandit' bank robbery suspect arrested.** A man dubbed the "Hipster Bandit" was arrested in Serra Mesa, California, July 14 after he allegedly robbed eight banks and attempted to rob two others in San Diego, Riverside, and Orange counties since November 2015.
Source: http://fox5sandiego.com/2016/07/14/hipster-bandit-bank-robbery-suspect-arrested/

Transportation Systems Sector

7. *July 15, Chattanooga Times Free Press* – (Tennessee) **Thousands of gallons of diesel fuel spilled, 3 injured after train hits heavy truck, derails in Lookout Valley.** Three locomotives and 10 rail cars on a Norfolk Southern train derailed July 14 after the train collided with a truck in Wauhatchie Pike in Tennessee, injuring 3 people, and spilling thousands of gallons of diesel fuel. Authorities closed several roads and intersections while crews worked to upright the derailed cars and repair the damaged track.
Source: http://www.timesfreepress.com/news/local/story/2016/jul/14/train-hits-semi-truck-derails-lookout-valley/375998/

8. *July 15, WAVY 10 Portsmouth* – (Virginia) **Man seriously hurt in motorcycle crash on Military Highway in Norfolk.** Military Highway in Norfolk, Virginia, was closed for several hours July 15 while crews worked to clear the wreckage after a motorcyclist lost control of his vehicle and crashed. The man was taken to a nearby hospital with serious injuries and officials believe alcohol and speed were factors in the crash.
Source: http://wavy.com/2016/07/15/serious-overnight-motorcycle-crash-in-norfolk/

9. *July 15, NJ.com* – (New Jersey) **All lanes of I-78 open after fatal tractor-trailer**

crash. All lanes of eastbound Interstate 78 in Tewksbury Township reopened July 15 following a fatal accident July 14 involving a semi-truck that left the driver dead and closed all lanes of a portion of the expressway for 6 hours before a single lane was reopened.
Source: http://www.nj.com/hunterdon/index.ssf/2016/07/all_lanes_of_i-78_open_after_fatal_tractor-trailer.html

10. *July 14, Houston Chronicle* – (Texas) **Houston Ship Channel reopened after spill of chemical compound shuts it down.** The Houston Ship Channel between the Lynchburg Ferry Crossing and Carpenters Bayou was closed for 2 hours July 14 due to a leak of about 500 gallons of benzene from the tanker Maritime Jingan. The leak was secured and only a small portion of the benzene entered the water.
Source: http://www.chron.com/news/houston-texas/houston/article/Part-of-Houston-Ship-Channel-closed-as-Coast-8378710.php

11. *July 14, San Luis Obispo Tribune* – (California) **Accidents involving SLO County drivers close two highways.** Highway 101 in San Luis Obispo County was closed for about 3 hours July 14 after a pickup truck collided with a concrete rail on the side of the bridge, blocking two lanes of traffic. Officials also closed southbound lanes of Highway 1 near Lompoc for approximately 4 hours while crews cleaned up an oil spill after a truck's fuel hoses dislodged.
Source: http://www.sanluisobispo.com/news/local/article89597537.html

12. *July 14, Twin Falls Times-News* – (Idaho) **9 train cars full of corn derail in Minidoka.** Authorities are investigating after nine Union Pacific train cars transporting corn derailed in Minidoka, Idaho, July 14.
Source: http://magicvalley.com/news/local/mini-cassia/train-cars-full-of-corn-derail-in-minidoka/article_d159fede-9320-51bb-8469-d453fc05e447.html

13. *July 14, WPLG 10 Miami* – (Florida) **Police say driver texting before fatal crash that closed US 1 for hours.** Southbound lanes of U.S. Highway 1 in Miami were closed for several hours July 14 while officials investigated the scene of a fatal accident involving two vehicles that left one person dead and a second person injured.
Source: http://www.local10.com/traffic/driver-texting-before-fatal-crash-that-closed-us-1-for-hours

Food and Agriculture Sector

14. *July 15, U.S. Department of Agriculture* – (Puerto Rico) **U.S. Cado Holdings, Inc. recalls imported siluriformes fish products distributed without meeting FSIS requirements.** U.S. Cado Holdings, Inc., expanded a previous recall July 14 to include an additional 1,650 pounds of its Deep Water Sea Food brand "Frozen Swai Fillets" products sold in 15-pound packages after the customer and import establishment notified Federal personnel that the products entered U.S. commerce without meeting Federal importation requirements concerning residue sampling and testing for imported siluriformes. There have been no confirmed reports of adverse reactions and the products were shipped to institutional locations in Puerto Rico.

Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-052-2016-release-expansion

15. *July 15, U.S. Department of Agriculture* – (National) **Haring Catfish, Inc., recalls siluriformes fish products due to possible adulteration.** Harings Catfish, Inc., issued a recall July 14 for approximately 21,521 pounds of its siluriformes catfish products sold in 3 variations due to potential gentian (crystal) violet contamination after Federal routine sampling results revealed the presence of gentian (crystal) violent in the products. There have been no confirmed reports of adverse reactions and the products were distributed to retail locations, hotels, restaurants, and institutions in six States.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-060-2016-release

16. *July 14, U.S. Food and Drug Administration* – (National) **Monogram Appetizers issues allergy alert on undeclared (egg) in Poppers Brand Mozzarella Cheese Sticks.** Monogram Foods issued a recall July 14 for approximately 5,000 cases of its Poppers Brand Mozzarella Cheese Sticks products due to mislabeling and undeclared egg after it was discovered during a routine quality check that the ingredient statement did not declare the presence of egg following a recent graphics change. No illnesses have been reported and the products were distributed to retail stores nationwide.
Source: http://www.fda.gov/Safety/Recalls/ucm511348.htm

17. *July 13, U.S. Department of Agriculture* – (National) **USDA announces changes to improve humane handling of veal calves.** The Food Safety and Inspection Service (FSIS) announced July 13 new rules that aim to improve the humane handling inspections at veal meat production facilities. The rule requires that veal calves brought to slaughter that cannot walk be humanely euthanized and prohibited from entering the food supply, improves compliance with the Humane Methods of Slaughter Act by encouraging improved treatment of veal calves, and improves inspection efficiency, among other regulations.
Source: http://www.fsis.usda.gov/wps/portal/fsis/newsroom/news-releases-statements-and-transcripts/news-release-archives-by-year/archive/2016/nr-071316-01

18. *July 13, California Department of Food and Agriculture* – (California) **Asian citrus psyllid quarantines in Merced and Monterey counties.** The California Department of Food and Agriculture issued a quarantine for Merced and Monterey counties July 13 after Asian citrus psyllid (ACP) was detected in the counties. The quarantine prohibits the movement of citrus and curry leaf tree nursery stock out of the quarantine zone, requires that all leaves and stems be removed from citrus fruits before transporting the fruits out of the zone, and prohibits residents with backyard citrus trees from transporting or sending citrus fruits or leaves, potted citrus trees, or curry leaves from the quarantine area.
Source: https://www.cdfa.ca.gov/egov/Press_Releases/Press_Release.asp?PRnum=16-026

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

19. *July 15, SecurityWeek* – (National) **Hundreds of flaws found in Philips Healthcare product.** Philips advised Xper Connect users to update their operating system (OS) to Microsoft Windows 2008-R2 and install Xper version 1.5 service pack 13 after Whitescope LLC and Synopsys researchers discovered 460 vulnerabilities in Philips Xper Information Management Connect, which include code injections, information exposure flaws, and resource management and numeric errors, among others, that can allow an attacker to compromise the system.
Source: http://www.securityweek.com/hundreds-flaws-found-philips-healthcare-product

20. *July 14, SC Magazine* – (California) **Ultrasound theft results in data breach at health care company Kaiser Permanente.** Kaiser Permanente's Northern California division announced July 13 that about 1,100 patients are known to be impacted by a data breach after 2 of its employees allegedly stole an unspecified number of ultrasound machines containing protected health information, with the intent of selling the machines. An investigation is ongoing.
Source: http://www.scmagazine.com/ultrasound-theft-results-in-data-breach-at-health-care-company-kaiser-permanente/article/509467/

Government Facilities Sector

21. *July 14, Arizona Republic* – (Arizona) **Lightning-ignited wildfire burns 3,000 acres at Grand Canyon.** Crews worked July 14 to contain the 3,057-acre Fuller Fire burning on the North Rim of the Grand Canyon in Arizona. Several trails and roads were closed as a precaution.
Source: http://www.azcentral.com/story/news/local/arizona/2016/07/15/lightning-ignited-fire-burns-3000-acres-grand-canyon/87114788/

For another story, see item **1**

Emergency Services Sector

Nothing to report

Information Technology Sector

22. *July 15, SecurityWeek* – (International) **New trojan helps attackers recruit insiders.** Researchers at Gartner Research and Diskin Advanced Technologies found a new trojan dubbed "Delilah" that uses social engineering and extortion to recruit insiders by collecting personal information and capturing video from the targeted user's webcam while instructing users to use virtual private networks (VPNs) and the Tor network in

order to manipulate or blackmail the targeted individual.
Source: http://www.securityweek.com/new-trojan-helps-attackers-recruit-insiders

23. *July 15, SecurityWeek* – (International) **IE exploit added to Neutrino after experts public PoC.** FireEye and Symantec researchers found that Neutrino exploit kit (EK) researchers use an Adobe Flash file to deliver exploits in order to profile a victim's system to determine which exploit to use after researchers published a proof-of-concept (PoC) exploit on two remote code execution (RCE) vulnerabilities that were patched by Microsoft in May. Researchers determined that the exploit added to Neutrino is identical to the one published, except for the code that runs after initial control.
Source: http://www.securityweek.com/ie-exploit-added-neutrino-after-experts-publish-poc

24. *July 14, Softpedia* – (International) **CryptXXX devs provide free decryption keys for some ransomware versions.** Bleeping Computer researchers released a category of users who could obtain a free decryption key by visiting the Tor-based payment sites of the CryptXXX ransomware after their files were encrypted by the ransomware using the ".crypz" and ".cryp1" file extensions at the end.
Source: http://news.softpedia.com/news/cryptxxx-devs-provide-free-decryption-keys-for-some-ransomware-versions-506333.shtml

25. *July 14, Softpedia* – (International) **Maxthon browser collects sensitive data even if users opt out.** Maxthon is investigating after Exatel and Fidelis Cybersecurity researchers found that the Maxthon Web browser collects sensitive information and sends it to its servers, even if the user opts out of the option due to an issue in the current implementation of User Experience Improvement Program (UEIP) that lets the browser manufacturer collect analytical information about how users utilize their product.
Source: http://news.softpedia.com/news/maxthon-browser-collects-sensitive-data-even-if-users-opt-out-506327.shtml

For additional stories, see items **19** and **26**

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. *July 14, Threatpost* – (International) **Cisco patches DoS flaw in NCS 6000 routers.** Cisco Systems released patches for two products addressing a Simple Network Management Protocol (SNMP) configuration management flaw in the Cisco ASR 5000 Series, prior to versions 19.4 and 20.1 that could allow a remote attacker to read and modify device configurations using the SNMP read-write community strings. The

second patch addresses a critical flaw in Cisco IOS XR for the Cisco Network Convergence System series router found in the management of system timer resources which could allow an attacker to remotely crash the router by sending a number of Secure Shell (SSH), Secure Copy Protocol (SCP), and Secure File Transfer Protocol (SFTP) management connections to an affected device.
Source: https://threatpost.com/cisco-patches-dos-flaw-in-ncs-6000-routers/119296/

Commercial Facilities Sector

27. *July 15, Brockton Enterprise* – (Massachusetts) **Raging 7-alarm fire destroys downtown Brockton warehouse.** The Bay State Restorations warehouse in Brockton, Massachusetts, sustained significant damage July 14 following a seven-alarm fire that prompted surrounding homes to be evacuated, cut power to the area, and forced a nearby Massachusetts Bay Transportation Authority (MBTA) commuter rail station on the Middleboro Line to close. One firefighter was injured and crews were working to contain the blaze.
Source: http://www.enterprisenews.com/news/20160714/raging-7-alarm-fire-destroys-downtown-brockton-warehouse

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