Homeland Security

Daily Open Source Infrastructure Report
18 August 2016

Top Stories

- City officials in Kalamazoo, Michigan, reported August 17 that more than 570,000 gallons of partially treated wastewater overflowed into the Kalamazoo River August 16 following severe storms in the area. – *Associated Press; WOOD 8 Grand Rapids* (See item **12**)

- The governor of California declared a state of emergency for San Bernardino County August 16 due to the 30,000-acre Blue Cut Fire that has forced the evacuation of more than 82,000 residents from an estimated 35,000 homes in the area. – *ABC News* (See item **15**)

- Nearly 1,200 inmates were evacuated from the Louisiana Correctional Institute for Women in St. Gabriel August 16 as a precautionary measure after floodwaters have continued to rise in the area. – *Baton Rouge Advocate* (See item **17**)

- Social Blade confirmed that its Website and forum were hacked in August after LeakedSource researchers discovered that the details of 13,009 of the forum's users and 273,806 of the Website's users' details were leaked, including password hashes and Internet Protocol (IP) addresses, among other information. – *SecurityWeek* (See item **20**)

Fast Jump Menu

Energy Sector

1. *August 17, Reuters* – (Louisiana) **Exxon Baton Rouge refinery shuts CDU due to flooding: sources.** ExxonMobil Corp. shut down a crude distillation unit at its Baton Rouge Refinery August 16 following severe flooding that disrupted operations at the refinery's liquefied petroleum gas (LPG) storage facility in Sorrento, Louisiana. Motive Enterprises, LLC also reduced staffing to essential personnel at its Covent, Louisiana refinery August 16 after a fire damaged the refinery's heavy oil hydrocracker August 11.
Source: http://www.reuters.com/article/us-refinery-operations-exxon-batonrough-idUSKCN10S0EK

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. *August 16, Newark Star-Ledger* – (New Jersey) **N.J. woman stole $89K in credit card scheme, cops say.** A former accountant at Forever Collectibles in Somerset, New Jersey, was charged August 16 for her role in an $89,000 credit card fraud scheme where she and a co-conspirator allegedly put the refunds from customers' returned items onto her family and friends' credit cards instead of the customers' cards between March and December 2015.
Source:
http://www.nj.com/somerset/index.ssf/2016/08/nj_woman_stole_89k_from_employer_in_credit_card_sc.html

3. *August 16, SecurityWeek* – (International) **Vawtrak banking trojan uses SSL pinning, DGA.** Fidelis security researchers discovered that a new version of the Vawtrak banking trojan includes a domain generation algorithm (DGA) that generates .ru domains using a pseudorandom number generator (PRNG) in the trojan's loader, uses Hypertext Transfer Protocol Secure (HTTPS) to protect command and control (C&C) communications, and leverages certificate pinning, or secure sockets layer (SSL) pinning that helps the malware evade detection by enterprise security solutions

that use their own certificates to intercept communications. Researches stated the trojan conducts checks based on the Common Name to identify the domain names associated with the certificate, and uses a public key from the initial inject carried out by the malware loader in order to ensure that no other certificates are accepted.
Source: http://www.securityweek.com/vawtrak-banking-trojan-uses-ssl-pinning-dga

Transportation Systems Sector

4. *August 17, WIS 10 Columbia*– (South Carolina) **Overturned truck spills gallons of asphalt on I-20.** Interstate 20 in Lexington County, South Carolina, was closed for several hours August 16 while crews worked to clear 4,800 gallons of asphalt that spilled after a semi-truck transporting tar overturned.
Source: http://www.live5news.com/story/32774545/overturned-truck-spills-gallons-of-asphalt-on-i-20

5. *August 17, Casa Grande Dispatch* – (Arizona) **Dramatic collision shuts down highway west of Casa Grande.** A two-vehicle crash involving a semi-truck and another vehicle prompted officials to close both lanes of Highway 84 near Stanfield, Arizona, for more than 2 hours August 16 while they investigated the scene of the crash. One driver was transported to an area hospital with injuries.
Source: http://www.trivalleycentral.com/casa_grande_dispatch/area_news/dramatic-collision-shuts-down-highway-west-of-casa-grande/article_26bdae58-63f6-11e6-85c2-83354e9e6e13.html

6. *August 17, WTVR 6 Richmond* – (Virginia) **Shattered glass across I-95 causes major delays in Petersburg.** Northbound lanes of Interstate 95 in Petersburg, Virginia, were closed for several hours August 16 while crews worked to clear the debris after a semi-truck dropped sheets of glass, leaving shattered glass on the roadway. No injuries were reported.
Source: http://wtvr.com/2016/08/16/shattered-glass-across-i-95-causing-major-delays-in-petersburg/

7. *August 16, Charleston Gazette-Mail* – (West Virginia) **One dead in fiery wreck on I-64 in Putnam County.** Interstate 64 eastbound near Teays Valley, West Virginia, was closed for several hours August 16 – August 17 after a multi-vehicle crash involving 4 semi-trucks and 2 other vehicles where a semi-truck traveling westbound crossed the median and struck another vehicle, causing a chain of collisions that left 1 person dead and sent 8 others to area hospitals.
Source: http://www.wvgazettemail.com/news/20160816/one-dead-in-fiery-wreck-on-i-64-in-putnam-county

8. *August 16, KEYT 3 Santa Barbara/KCOY 12 Santa Maria/KKFX 24 San Luis Obispo* – (California) **Emergency plane landing under investigation at the Santa Barbara airport.** A United Airlines flight en route to San Francisco International Airport from Los Angeles International Airport was forced to make an emergency landing in Santa Barbara, California, August 15 after the flight crew noticed the odor of smoke in the cockpit. The cause of the odor remains investigation.

Source: http://www.keyt.com/news/emergency-plane-landing-under-investigation-at-the-santa-barbara-airport/41234226

9. *August 16, Vacaville Reporter* – (California) **Davis woman dies in vehicle collision.** Pedrick Road in Dixon, California, was closed for approximately 3 hours August 16 while officials investigated the cause of a 2-vehicle accident that left 1 person dead and 2 others injured after a vehicle crossed the center line and struck another vehicle head-on.
Source: http://www.thereporter.com/general-news/20160816/davis-woman-dies-in-vehicle-collision

10. *August 16, KSAT 12 San Antonio* – (Texas) **Jackknifed 18-wheeler snarls traffic on I-37 southbound near Loop 410 interchange.** All lanes of Interstate 37 in San Antonio, Texas, were closed for several hours August 16 while HAZMAT crews worked to clear the wreckage after a semi-truck hit a guardrail and overturned, causing diesel to spill on the roadway. One person was sent to an area hospital with non-life threatening injuries.
Source: http://www.ksat.com/traffic/traffic-incidents/jackknifed-18-wheeler-closes-i-37-southbound-at-410-interchange

For another story, see item **23**

Food and Agriculture Sector

11. *August 16, U.S. Department of Labor* – (Texas) **Amputation at Tyson Foods exposes chemical, fall, fire hazards at Texas plant.** The Occupational Safety and Health Administration cited Tyson Foods, Inc. with 2 repeated and 15 serious violations August 15 after an employee's finger was amputated while working on an unguarded conveyer belt, prompting an investigation at the Center, Texas facility, which revealed that the company failed to protect employees from high levels of carbon dioxide and peracetic acid, failed to provide personal protective equipment, and failed to install proper safety guards on moving machine parts. Proposed penalties total $263,498.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=32997

For another story, see item **22**

Water and Wastewater Systems Sector

12. *August 17, Associated Press; WOOD 8 Grand Rapids* – (Michigan) **Warning issued for Kalamazoo River after wastewater overflow.** City officials in Kalamazoo, Michigan, issued a water advisory August 17 warning people to avoid a 5-mile stretch of the Kalamazoo River after severe rains caused more than 570,000 gallons of partially treated wastewater to overflow into the river August 16.
Source: http://www.ccenterdispatch.com/news/state/article_fa7706ec-fb46-51c6-be51-ec4d4939a6d6.html

13. *August 16, DurandNow.com* – (Mississippi) **Sewage overflow in Durand due to flooding.** Shiawassee Health Department officials announced August 16 that approximately 20,000 gallons of partially treated wastewater overflowed from the Durand Wastewater Treatment Plant in Duran, Mississippi, into the Holly Drain, which flows into the Shiawassee River near Vernon following heavy rainfall in the area.
    Source: http://www.durandnow.com/Stories-Sewage-Overflow-In-Durand-Due-to-Flooding.html

For another story, see item **1**

Healthcare and Public Health Sector

14. *August 17, Easton Express-Times* – (New Jersey) **'Minor' acid spill forces evacuation of N.J. medical office.** A Coordinated Health-managed facility in Lopatcong Township, New Jersey, was evacuated August 16 and closed until August 17 due to a phenol leak after a partially filled 20-ounce bottle of the chemical was dropped on an exam room floor. HAZMAT crews worked to contain the spill and 12 people were treated for exposure to the acid.
    Source:
    http://www.lehighvalleylive.com/warren-county/index.ssf/2016/08/acid_spill_forces_evacuation_o.html

Government Facilities Sector

15. *August 17, ABC News* – (California) **Devastating southern California wildfire grows to 30,000 acres, 0% contained.** The governor of California declared a state of emergency for San Bernardino County August 16 due to the 30,000-acre Blue Cut Fire that has forced the evacuation of more than 82,000 residents from an estimated 35,000 homes in the area.
    Source: http://abcnews.go.com/US/massive-southern-california-wildfire-covers-30000-acres-contained/story?id=41452228

Emergency Services Sector

16. *August 16, KCCI 8 Des Moines* – (National) **Nationwide warrant issued for escaped inmate.** Authorities issued a nationwide search warrant August 16 for an inmate who escaped from the Warren County Jail in Indianola, Iowa, August 14 while a correctional officer was delivering medication to inmates.
    Source: http://www.kcci.com/news/inmate-escapes-from-warren-county-jail-authorities-say/41203120

17. *August 16, Baton Rouge Advocate* – (Louisiana) **DOC: 1,200 prisoners to evacuate women's lockup in St. Gabriel as precaution.** Nearly 1,200 inmates were evacuated from the Louisiana Correctional Institute for Women in St. Gabriel August 16 as a precautionary measure after floodwaters have continued to rise in the area. Officials stated roughly 600 inmates were evacuated from the Livingston Parish Detention

Center and sent to 4 other State prisons the weekend of August 13 due to rising floodwaters.
Source: http://www.theadvocate.com/baton_rouge/news/article_b9854430-63ce-11e6-aa1c-dbffc3042ae7.html

18. *August 16, KHBS 40 Fort Smith/KHOG 29 Fayetteville* – (Arkansas) **Rogers officer's AR-15, magazines, other items, stolen from police car.** The chief of police in Rogers, Arkansas, reported August 16 that a weapon, loaded magazines, handcuffs, and a bullet resistant vest, among other items, were stolen from an unmarked police officer's vehicle at his home in Rogers.
Source: http://www.4029tv.com/news/rogers-officers-ar15-magazines-other-items-stolen-from-police-car/41229070

Information Technology Sector

19. *August 17, SecurityWeek* – (International) **Backdoor abuses TeamViewer to spy on victims.** Dr. Web security researchers discovered a backdoor trojan, dubbed BackDoor.TeamViewrENT.1 and distributed under the name "Spy-Agent" was installing legitimate TeamViewer components on a compromised device to spy on victims in the U.S., Europe, and Russia, steal victims' personal information, and to install other malicious programs on a device. Researchers found that the trojan disables error messaging for the TeamViewer process, changes the attributes of its files and the TeamViewer files to "system," "hidden," and "ready only", and kills the TeamViewer process if the Microsoft Windows Task Manager or Process Explorer are detected in order to hide its presence on an infected device.
Source: http://www.securityweek.com/backdoor-abuses-teamviewer-spy-victims

20. *August 17, SecurityWeek* – (International) **User data leaked from analytics company Social Blade.** Social Blade, a data provider for YouTube, Twitch, and Instagram accounts, confirmed that its Website and forum were hacked in August after LeakedSource researchers discovered that the details of 13,009 of the forum's users and 273,806 of the Website's users' details were leaked, including email addresses, usernames, password hashes, and Internet Protocol (IP) addresses, among other information, after a malicious actor obtained a partial database dump by exploiting a vulnerability in the forum software. Social Blade reset all user passwords and shut down its forum.
Source: http://www.securityweek.com/user-data-leaked-analytics-company-social-blade

21. *August 16, Softpedia* – (International) **Chrome and Firefox attached by simple URL spoofing bug that facilitates phishing.** A security researcher discovered a flaw affecting security features in Google Chrome and Mozilla Firefox can be exploited to spoof Universe Resource Locators (URLs) in the browser address bar after finding that Web browsers handle URLs written with mixed right-to-left (RTL) (Arabic) and left-to-right (LTR) (Roman) characters incorrectly, which confuses the browsers and forces them to switch parts of the URL, thereby tricking the user into thinking that they are accessing a different Website than the one they are on. The researcher stated a hacker

running a phishing site can add a few Arabic characters onto a server's Internet Protocol (IP) to change the domain of a legitimate Website and embed this URL in spam email, short message service (SMS), or instant messaging (IM) message in order to redirect an user to the malicious actor's server.
Source: http://news.softpedia.com/news/chrome-and-firefox-affected-by-simple-url-spoofing-bug-that-facilitates-phishing-507369.shtml

For another story, see item **3**

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 item **20**

Commercial Facilities Sector

22. *August 16, WFMJ 21 Youngstown* – (Ohio) **Cause of feed mill fire in Alliance under investigation.** Schott Feed and Supply, Inc., in Alliance, Ohio, was considered a total loss August 16 following a fire that destroyed the main building and caused significant damage to surrounding structures. Officials were working to determine the cause and extent of the damage.
Source:
http://www.wfmj.com/story/32770036/cause-of-feed-mill-fire-in-alliance-under-investigation

23. *August 15, WGAL 8 Lancaster* – (Pennsylvania) **Huge business fire causes half a million dollars in damage.** A building housing multiple businesses in Paradise Township, Pennsylvania, was considered a total loss August 15 following a fire that prompted the shutdown of a portion of Route 30 between McIlvaine Road and Slaymaker Road for nearly 8 hours. The cause of the fire remains under investigation and officials estimated the fire caused $500,000 in damage.
Source: http://www.wgal.com/news/crews-battling-overnight-business-fire-in-lancaster-county/41203396

Dams Sector

Nothing to report

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

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.