Daily Open Source Infrastructure Report
15 August 2016

Top Stories

- Security researchers discovered two remote system attacks capable of unlocking millions of cars including one attack that targets Volkswagen Group cars and involves recovering the keys from electronic control units. – *Help Net Security* (See item **4**)
- Two Houston residents were arrested August 11 for their roles in a $650,000 credit card fraud scheme where the duo and another co-conspirator allegedly used 2 Houston-area businesses to steal the identities of at least 12 customers in order to obtain 116 credit cards. – *KTRK 13 Houston* (See item **7**)
- Bon Secours Health System announced August 12 that approximately 665,000 patients were notified of a data breach after a third-party company inadvertently left confidential files accessible on the Internet from April 18 – 21. – *WTKR 3 Norfolk* (See item **20**)
- Authorities are investigating August 11 after the U.S. Forest Service discovered a 5-acre illegal marijuana operation in Pike National Forest in Jefferson, Colorado, consisting of about 18,300 plants. – *Colorado Springs Gazette* (See item **22**)

Fast Jump Menu

Energy Sector

1. *August 12, Associated Press* – (Michigan) **Crews extinguish fire at Michigan power plan; no injuries.** The DTE Energy Co. facility in East China Township, Michigan, was evacuated and closed until further notice August 11 following a fire that began after a coal-fired generation unit caught fire. Officials closed surrounding roads while they worked to contain the blaze and no injuries were reported.
   Source: http://abcnews.go.com/US/wireStory/crews-work-overnight-battling-fire-michigan-power-plant-41322326

2. *August 11, Baton Rouge Advocate* – (Louisiana) **Motiva oil refinery fire is out, no injuries or fatalities reported, according to St. James officials.** Authorities are investigating the cause of a fire at the Motiva Enterprises, LLC, facility in St. James, Louisiana, that prompted the evacuation of approximately 1,400 employees for over 4 hours August 11 while crews worked to contain the blaze.
   Source: http://www.theadvocate.com/baton_rouge/news/article_17dcedc6-5fdd-11e6-8166-a3233d12f46b.html

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

3. *August 11, Columbia State* – (South Carolina) **Up to 170 Westinghouse workers to temporarily lose jobs.** Westinghouse Electric Company voluntarily shut down its nuclear fuel assembly and component facility in Columbia, South Carolina, the week of August 8 after the U.S. Nuclear Regulatory Commission (NRC) was notified July 14 of an accumulation of excessive amounts of uranium-bearing material in an air scrubber. NRC officials reported to the facility August 1 to investigate the build-up.
   Source: http://www.thestate.com/news/business/article95065072.html

Critical Manufacturing Sector

4. *August 11, Help Net Security* – (International) **Hundreds of millions of cars can be easily unlocked by attackers.** Security researchers discovered two remote system attacks capable of unlocking millions of cars including one attack that targets Volkswagen Group cars and involves recovering the cryptographic algorithms and keys from electronic control units, which allows an attacker to clone the signal to open the vehicle, and another attack that exploits the cryptographically weak cipher in Hitag2 rolling code scheme used by manufacturers like Chevrolet and Ford, among others, to unlock the vehicle.
   Source: https://www.helpnetsecurity.com/2016/08/11/cars-easily-unlocked-attackers/

5. *August 11, TheCarConnection.com* – (National) **2016 Honda Civic recalled to fix lighting flaw.** Honda Motor Company, Ltd., issued a recall August 11 for 11,846 of its 2016 model year Honda Civic Coupe vehicles sold in the U.S. due to a potential

lighting problem where the circuit boards that control the rear side marker light-emitting diode (LED) lights may have been damaged during shipping, thereby making it more difficult to see in low-light conditions and increasing the risk of a crash.
Source: http://www.thecarconnection.com/news/1105502_2016-honda-civic-recalled-to-fix-lighting-flaw

6. *August 11, U.S. Department of Labor*– (Illinois) **OSHA finds Illinois trailer manufacturer continues to expose workers to risk of injuries from machine, welding hazards.** The Occupational Safety and Health Administration cited Dierzen Sales, Ltd., with one willful, one repeat, and five serious violations August 5 following a March inspection at its Newark, Illinois facility which revealed that the company failed to evaluate powered industrial vehicle operators as required, failed to cover electrical boxes and openings, and exposed employees to fall and trip hazards, among other violations. Proposed penalties total $153,791.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=32991

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

7. *August 11, KTRK 13 Houston* – (Texas) **Police bust identity theft scheme that netted $650K.** Two Houston residents were arrested August 11 for their roles in a more than $650,000 credit card fraud scheme where the duo and another co-conspirator allegedly used 2 southwest Houston businesses, Lagos Island Café and Lace Warehouse and African Fashions, to steal the identities of at least 12 customers in order to apply for and obtain 116 credit cards from 8 different Houston-area financial institutions. The charges allege that one of the co-conspirators ran the credit cards under a fraudulent business name, Sleek Auto Sales and deposited the funds into a personal bank account.
Source: http://abc13.com/news/police-bust-identity-theft-scheme-that-netted-$650k/1466692/

Transportation Systems Sector

8. *August 12, WITI 6 Milwaukee* – (Wisconsin) **One person killed following car vs. semi crash near Whitewater.** Highway 12 in Whitewater, Wisconsin, was closed for approximately 3 hours August 11 following a two-vehicle crash involving a semi-truck and another vehicle that left one person dead.
Source: http://fox6now.com/2016/08/11/one-person-killed-following-car-vs-semi-crash-near-whitewater/

9. *August 12, New Haven Register* – (Connecticut) **Driver killed in New Haven sweeper truck crash.** The southbound Exit 6 off-ramp from Interstate 91 and a portion of

Willow Street in New Haven, Connecticut, were closed for approximately 3 hours August 11 while crews worked to clear the wreckage after a street sweeper crashed on the ramp and overturned, killing the driver.
Source: http://www.nhregister.com/general-news/20160811/driver-killed-in-new-haven-sweeper-truck-crash

10. *August 12, WLTX 19 Columbia* – (South Carolina) **3 taken to hospital after multi-vehicle accident on I-95.** Northbound lanes of Interstate 95 in Santee, South Carolina, were closed for several hours August 11 – August 12 while crews worked to clear the wreckage from a 4-vehicle accident that caused a semi-truck transporting logs to overturn and spill its load on the highway. Three people were transported to an area hospital with injuries.
Source: http://www.wltx.com/news/local/multi-vehicle-accident-shuts-down-i-95-causes-injuries/295689309

11. *August 12, KSLA 12 Shreveport* – (Texas) **I-30 reopened after fiery fatal pileup near Texarkana.** Westbound lanes of Interstate 30 near Texarkana, Texas were closed for about 7 hours August 11 – August 12 while crews worked to clear the wreckage from a multi-vehicle pileup that caught fire. One person was killed and two others were transported to an area hospital with injuries.
Source: http://www.ksla.com/story/32741915/traffic-alert-multiple-wrecks-prompt-closure-of-i-30-wb-near-texarkana

12. *August 12, WBZ 4 Boston* – (Massachusetts) **Mass pike shut down in Charlton following crash involving two trucks.** Two semi-trucks collided on Massachusetts Pike in Charlton, Massachusetts, August 12, forcing the closure of the eastbound lanes for several hours while crews worked to clear the wreckage and officials investigated the scene.
Source: http://boston.cbslocal.com/2016/08/12/mass-pike-shut-down-in-charlton-following-crash-involing-two-trucks/

13. *August 12, KOTV 6 Tulsa* – (Oklahoma) **OHP releases name of man killed walking on Tulsa highway.** Oklahoma Highway Patrol closed eastbound lanes of Interstate 44 in east Tulsa, Oklahoma, for 4 hours August 12 after a pedestrian was fatally struck by a vehicle.
Source: http://www.newson6.com/story/32744431/pedestrian-killed-walking-on-tulsa-interstate-highway

14. *August 12, Washington Post* – (South Dakota) **'It got really rocky': 24 hospitalized after JetBlue plane ran into severe turbulence.** At least 22 passengers and 2 crew members were taken to Rapid City Regional Hospital in South Dakota and treated for minor injuries August 11 after JetBlue flight 429 en route from Boston to Sacramento was forced to make an emergency landing in Rapid City due to extreme turbulence.
Source: https://www.washingtonpost.com/news/morning-mix/wp/2016/08/12/it-got-really-rocky-24-hospitalized-after-jetblue-plane-ran-into-severe-turbulence/

15. *August 11, Syracuse Post-Standard* – (New York) **Dump truck driver stops to grab**

loose tire, gets hit by van in Syracuse. A portion of Interstate 81 northbound in Syracuse, New York, was closed for about 2 hours August 11 after a driver was struck by another vehicle while attempting to grab a tire fell off of his vehicle. Both drivers were taken to Upstate University Hospital with injuries.
Source:
http://www.syracuse.com/crime/index.ssf/2016/08/dump_truck_driver_tries_to_grab_loose_tire_gets_hit_by_van_in_syracuse.html

16. *August 11, Longview Daily News* – (Oregon) **Fleeing driver killed in Highway 30 crash.** Both directions of Highway 30 in St. Helens, Oregon, were closed for several hours August 11 after a car fleeing from local police crashed into another vehicle, killing one person and sending another to an area hospital with serious injuries.
Source: http://tdn.com/news/local/highway-closed-for-several-hours-at-st-helens-city-limits/article_7daf5060-c577-523b-87fa-6e00f8ed8dd5.html

17. *August 11, Columbia Daily Tribune* – (Missouri) **Centralia man killed in crash near Hallsville.** Highway 124 near Hallsville, Missouri, was closed for several hours August 11 while officials investigated a two-vehicle accident after a dump truck and another vehicle collided, leaving one driver dead and the other injured.
Source: http://www.columbiatribune.com/news/local/one-dead-in-highway-crash-near-hallsville/article_097d2e4e-6962-541e-b84b-8bed7f16d3a7.html

18. *August 11, Meridian Star* – (Mississippi) **UPS driver killed, 2 injured in I-20 truck accident in Newton County.** One person was killed following a collision involving three semi-trucks that prompted the closure of Interstate 20 in Newton County, Mississippi, for several hours August 11.
Source: http://www.meridianstar.com/news/local_news/ups-driver-killed-injured-in-i--truck-accident-in/article_b34eac09-bd00-5021-85cc-916a3471cda5.html

Food and Agriculture Sector

19. *August 12, Food Safety News* – (National) **Baking mixes recalled nationwide because of E. coli in flour.** Rabbit Creek Products issued a recall August 12 for its baking mix products sold under 31 brands due to a potential E. coli O121 contamination after the company's flour supplier, General Mills, Inc., recalled the products due to an ongoing E.coli outbreak linked to its flour products that has sickened 46 people across 21 States since December 2015. No illnesses have been reported and the products were distributed online and to retail locations nationwide.
Source:
http://www.foodsafetynews.com/2016/08/baking-mixes-recalled-nationwide-because-of-e-coli-in-flour/#.V63Qw_mANBc

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

20. *August 12, WTKR 3 Norfolk* – (National) **665,000 Bon Secours patients exposed to data breach.** Bon Secours Health System announced August 12 that approximately 665,000 patients were notified of a data breach after a third-party company inadvertently left files containing patients' names, health insurance identification numbers, and Social Security numbers, among other information, accessible on the Internet while attempting to adjust their network settings from April 18 – 21. Officials do not believe the information was misused.
Source:
http://wtkr.com/2016/08/12/665000-bon-secours-patients-exposed-to-data-breach/

21. *August 12, U.S. Food and Drug Administration* – (National) **Ton Shen Health recalls "DHZC-2 Tablet" because of possible health risk.** Ton Shen Health Chicago Acupuncture issued a recall August 11 for its DHZC-2 tablets after samples of the tablets revealed elevated lead levels. One illness has been reported in connection with the products which were sold in retail stores in Chicago and distributed through mail order to other States.
Source:
http://www.fda.gov/Safety/Recalls/ucm516439.htm

Government Facilities Sector

22. *August 11, Colorado Springs Gazette* – (Colorado) **5 acres of marijuana found in Pike National Forest.** Authorities are investigating August 11 after the U.S. Forest Service discovered a 5-acre illegal marijuana grow operation in Pike National Forest in Jefferson, Colorado, consisting of about 18,300 plants and 2,000 pounds of infrastructure including irrigation pipes, chemicals, and fertilizer, among other materials.
Source: http://gazette.com/5-acres-of-marijuana-found-in-pike-national-forest/article/1582517

23. *August 11, KFSN 30 Fresno* – (California) **Mineral Fire grows to nearly 7,050 acres, 25 percent contained.** Crews reached 25 percent containment August 11 of the 7,050-acre Mineral Fire burning near Coalinga, California.
Source: http://abc30.com/news/mineral-fire-grows-to-6952-acres-15-percent-contained/1465577/

24. *August 11, KATU 2 Portland* – (Oregon) **Evacuation at Polk Co. courthouse when suspicious bag left on steps.** The Polk County Circuit Court in Dallas, Oregon, was evacuated for about 2 hours August 11 after a suspicious bag was found on the front steps of the facility. Officials scanned the bag and deemed the area safe after no threat was found.
Source: http://katu.com/news/local/evacuation-at-polk-county-courthouse-when-suspicious-bag-left-on-steps

Emergency Services Sector

Nothing to report

Information Technology Sector

25. *August 12, Softpedia* – (International) **Locky ransomware uses vulnerable PHP forms for spam distribution.** Researchers from Cisco's OpenDNS team discovered that the group behind the Locky ransomware is leveraging security flaws in a PHP: Hypertext Preprocessor (PHP)-based Web-to-email service that allows the cybercriminals to brute-force the Web from and make it send a message with the Locky payload attached to any email address due to a vulnerability in a PHP contact form script. Researchers advised users to update their PHP Web-to-email form to the latest version to fix the problem.
Source: http://news.softpedia.com/news/locky-ransomware-uses-vulnerable-php-forms-for-spam-distribution-507246.shtml

26. *August 12, SecurityWeek* – (International) **Microsoft patches flaw related to "malicious butler" attack.** Microsoft released a patch addressing a serious Windows authentication bypass vulnerability, dubbed a "remote malicious butler" attack after researchers discovered the flaw can be leveraged remotely to bypass authentication on the Windows login screen, and found that in a patched version of Windows, a device's password could be changed if the rogue domain controller was disconnected in the middle of the password reset process. Researchers stated the patch addresses both the local evil maid attack and the remote butler version of the attack.
Source: http://www.securityweek.com/microsoft-patches-flaw-related-malicious-butler-attack

For another story, see item **4**

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

27. *August 12, SecurityWeek* – (International) **D-Link patches critical flaw in DIR routers.** D-Link released firmware updates for several of its DIR model routers to resolve a critical stack-based buffer overflow after a researcher discovered the flaw was affecting a function responsible for validating session cookies that could be exploited for arbitrary code execution. D-Link researchers were working to patch the flaw in its DIR-817 Rev. Ax and DIR-818L Rev. Bx router models.
Source: http://www.securityweek.com/d-link-patches-critical-flaw-dir-routers

Commercial Facilities Sector

28. *August 10, Hudson County Jersey Journal* – (New Jersey) **Residents displaced from 9 apartments after downtown Jersey City fire: official.** A 3-alarm fire at a downtown Jersey City, New Jersey, apartment complex August 10 caused significant damage to 2 businesses on the ground floor of the complex and left the residents of 9 units displaced after the fire reportedly began following a short in an electric circuit in one of the unit's bathrooms.
Source: http://www.nj.com/hudson/index.ssf/2016/08/residents_displaced_from_9_apartments_after_downto.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