Homeland Security

Daily Open Source Infrastructure Report 19 August 2015

Top Stories

- Recently published research from a 2013 report revealed that weaknesses in the Megamos Crypto system could be leveraged via “close-range wireless communication” attacks to remotely unlock over 100 vehicle models. – *The Guardian* (See item **2**)
- A Romanian man pleaded guilty August 17 to his role in an international ATM skimming operation involving 4,583 stolen bank card numbers, skimming devices, and about $15,000 in stolen funds. – *U.S. Attorney’s Office Eastern District of Pennsylvania* (See item **5**)
- The New York Metropolitan Transportation Authority shut down Long Island Rail Road service in Bethpage August 16 after a small plane crashed onto the tracks. – *WNBC 4 New York* (See item **9**)
- The U.S. Internal Revenue Service announced August 17 that an additional 220,000 taxpayers may have had their account information breached in a May incident involving thefts targeting the agency’s “Get Transcript” system. – *Associated Press* (See item **16**)

Fast Jump Menu

Energy Sector

Nothing to report

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

1. *August 18, WRDW 12 Augusta* – (South Carolina) **Lockdown of SRS is lifted after possible security threat.** The Savannah River Site in Aiken, South Carolina, reopened August 17 following a 3-hour lockdown due to a potential security threat when electronic and canine tests detected explosive residue in a Coca-Cola truck. Authorities searched the vehicle and cleared the scene once nothing suspicious was found.
   Source: http://www.wrdw.com/home/headlines/Savannah-River-Site-322079422.html

Critical Manufacturing Sector

2. *August 18, The Guardian* – (International) **Security flaw affecting more than 100 car models exposed by scientists**. Research published from a 2013 report by British and Dutch academics revealed weaknesses in the Swiss-made Megamos Crypto system used to prevent certain Audi, Citroën, Fiat, Honda, Volvo, and Volkswagen vehicles' engines from starting when a remote key is not present, in which a third party could use "close-range wireless communication" attacks to disable the system and steal the vehicle.
   Source: http://www.theguardian.com/technology/2015/aug/18/security-flaw-100-car-models-exposed-scientists-volkswagen-suppressed-paper

Defense Industrial Base Sector

3. *August 17, Los Angeles Times* – (California) **Jet involved in midair collision was on mission to test Navy radar.** BAE Systems officials reported August 17 that a Sabreliner jet involved in an August 16 midair collision over Otay Mesa was carrying 3 BAE employees and a subcontractor returning to Brown Field from a U.S. Navy radar system test. The crash killed all aboard the Sabreliner as well as the pilot of the Cessna.
   Source: http://www.latimes.com/local/lanow/la-me-ln-jet-collision-navy-20150817-story.html

4. *August 17, Reuters* – (National) **First flight of Boeing's military tanker delayed by a month.** Boeing Co., officials announced August 17 that the first flight of the U.S. Air Force's new KC-46 Pegasus tanker would be delayed by a month after an uncompliant chemical substitute was run through the aircraft's fuel system.
   Source: http://www.reuters.com/article/2015/08/17/boeing-tanker-idUSL1N10S1ZG20150817

Financial Services Sector

5. *August 17, U.S. Attorney's Office Eastern District of Pennsylvania* – (International) **Romanian National admits to international ATM skimming scheme.** A Romanian citizen pleaded guilty in Philadelphia August 17 to his role in an international scheme in which conspirators allegedly placed skimming devices on ATMs in Europe and the U.S., and withdrew funds from compromised accounts. Authorities arrested the man in South Carolina and found a total of 4,583 stolen bank card numbers, ATM skimming devices, and about $15,000 in stolen funds.
   Source: https://www.fbi.gov/philadelphia/press-releases/2015/romanian-national-admits-to-international-atm-skimming-scheme

6. *August 17, Oak Lawn Patch* – (Illinois) **FBI intensifies search for serial bank robber dubbed 'Midday Bandit'.** The FBI is offering $10,000 for information leading to the capture and arrest of a suspect dubbed the "Midday Bandit", who allegedly robbed 8 Chicago-area banks and attempted to rob 2 others since June 2014, with the most recent incident occurring at a U.S. Bank branch in Oak Park August 3.
   Source: http://patch.com/illinois/oaklawn/fbi-intensifies-search-serial-bank-robber-dubbed-midday-bandit

For another story, see item **16**

Transportation Systems Sector

7. *August 18, WTVT 13 Tampa Bay* – (Florida) **Man killed when Amtrak collides with car in Auburndale.** An Amtrak train was delayed for over 3 hours August 17 while officials investigated the scene after a train collided with a vehicle and killed one person. Police believe that the driver did not see the train coming at the crossing.
   Source: http://www.myfoxtampabay.com/story/29807324/1-person-killed-when-amtrak-collides-with-car-in-auburndale

8. *August 17, St. Louis Post-Dispatch* – (Missouri) **Tractor-trailer crash closes I-55 southbound at I-255.** The southbound lanes of Interstate 55 were shut down at Interstate 27 in St. Louis County, Missouri, for about 4 hours August 17 while crews cleared the scene of an overturned semi-truck that blocked most of the lanes.
   Source: http://www.stltoday.com/news/local/metro/commuter-alert-i--southbound-closed-near-i--delays/article_01d97935-e708-53f2-98b6-2699f55b4f4a.html

9. *August 17, WNBC 4 New York* – (New York) **1 dead, 1 hurt in plane crash on Long Island Rail Road tracks.** The New York Metropolitan Transportation Authority shut down service on the Long Island Rail Road at the site in Bethpage for most of the day August 16 after a small plane crashed onto the railroad tracks, killing the pilot and injuring a passenger. The plane took off from Gabreski Airport in Westhampton Beach and was headed to Morristown, New Jersey.
   Source: http://www.nbcnewyork.com/news/local/NY-Long-Island-Plane-Crash-Casualties-LIRR-Service-Suspended-321986792.html

10. *August 16, WDAY 970 AM Fargo; WDAZ 8 Devils Lake* – (North Dakota) **Interstate 29 shut down, traffic diverted, after head-on crash.** Interstate 29 near Manvel was shut down for several hours August 16 while crews investigated the cause of an accident that involved a semi-truck and a vehicle and sent 1 person to a local hospital.
    Source: http://www.wday.com/news/north-dakota/3818515-interstate-29-shut-down-traffic-diverted-after-head-crash

For another story, see item **17**

Food and Agriculture Sector

11. *August 18, U.S. Department of Agriculture* – (International) **Givaudan Flavors Corporation recalls beef tallow products produced without benefit of import inspection.** Florence, Kentucky-based Givaudan Flavors Corporation issued a recall for approximately 3,950 pounds of beef tallow products August 17, packaged in 50-pound bags and manufactured by York Foods Pty. Limited, Australia, after the items were not presented for inspection at the U.S. point of entry. The products were used in the production of a powdered beef flavor and then shipped to locations in Ohio and Texas for further processing.
    Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-112-2015-release

Water and Wastewater Systems Sector

12. *August 18, Philly.com* – (Pennsylvania) **Delco agency pays $1.3M over polluting claim.** The Delaware County Regional Water Authority agreed to pay nearly $1.4 million in a settlement announced August 17 with the U.S. Department of Justice, the U.S. Environmental Protection Agency, and the Commonwealth of Pennsylvania, for allegedly letting untreated wastewater flow into Ridley Creek, Chester Creek, and the Delaware River, endangering residents of Delaware County and parts of Chester County.
    Source:
    http://www.philly.com/philly/news/local/20150818_Delco_agency_pays__1_4M_over_polluting_claim.html

13. *August 17, WGRZ 2 New York* – (New York) **Boil and conserve water alert issued for Silver Creek residents.** The Chautauqua County Health Department issued a boil and conserve water alert August 17 for about 2,200 residents in Silver Creek following 2 water main breaks. Officials were continuing to test water to ensure its safety.
    Source: http://www.wgrz.com/story/news/local/2015/08/17/boil-and-conserver-water-alert-issued--silver-creek-residents/31858255/

Healthcare and Public Health Sector

14. *August 17, Reuters* – (International) **FDA warns makers of superbug-prone devices over testing violations.** The U.S. Food and Drug Administration issued warning letters to Olympus Corp Pentax Medical and Fujifilm Holdings Corp., August 12 citing the

manufacturers with several violations regarding improper cleaning, sterilization, and testing procedures of their medical devices following inspections at U.S. and international facilities. The devices were linked to recent superbug outbreaks at several U.S. hospitals.
Source: http://www.reuters.com/article/2015/08/17/us-health-fda-duodenoscope-idUSKCN0QM1PG20150817

15. *August 17, KUSA 9 Denver* – (Colorado) **Colorado Medicaid sends personal info to wrong addresses.** The Colorado Department of Health Care Policy and Financing reported August 17 that the protected personal and health information of 1,622 households was inadvertently mailed to the wrong addresses. The department contacted individuals involved and asked that the letters be returned or destroyed.
Source: http://www.9news.com/story/news/local/2015/08/17/personal-medicaid-information-sent--wrong-addresses/31862221/

Government Facilities Sector

16. *August 18, Associated Press* – (National) **IRS: Computer breach bigger than first thought; 334,000 victims.** The U.S. Internal Revenue Service announced August 17 that an additional 220,000 taxpayers may have had their account information breached in an incident disclosed in May where thieves stole tax information after accessing the agency's "Get Transcript" system where taxpayers can get tax returns and filings from previous years. The agency stated that it believes the total number of potential victims rose to 334,000 while it continues to investigate the breach.
Source: http://www.tulsaworld.com/business/consumer/irs-computer-breach-bigger-than-first-thought-victims/article_51aba05f-b15e-5df4-acc3-387bdf675fb7.html

17. *August 17, Fresno Bee; Associated Press* – (California) **Rough fire east of Fresno surges to 20,979 acres.** The 20,979-acre Rough Fire in the Sierra National Forest prompted authorities August 17 to rate the air quality as unhealthy in Fresno and Tulare counties, to order a fire evacuation warning for the Black Rock Reservoir area and Cedar Grove, and to shut down a portion of the Highway 180 past the Hume Lake turnoff.
Source: http://www.fresnobee.com/news/local/article31308059.html

18. *August 17, Santa Rosa Press Democrat* – (California) **Jerusalem Fire in Lake County now 90 percent contained.** Crews reached 90 percent containment August 17 of the 25,118-acre Jerusalem Fire burning in Lake County, California. Firefighters worked to surround the blaze with fire lines by August 21 after the fire destroyed 9 homes and 18 outbuildings.
Source: http://www.pressdemocrat.com/news/4352806-181/jerusalem-fire-in-lake-county

19. *August 17, KFSM 5 Fort Smith* – (Arkansas) **A dozen students treated after school bus crash.** Twelve Springdale School District students were injured August 17 after a vehicle hit a school bus head-on south of Arkansas Highway 412 on Sonora Road in Washington County.

Source: http://5newsonline.com/2015/08/17/a-dozen-students-treated-after-school-bus-crash/

20. *August 17, Associated Press* – (Washington) **National Guard mobilized as wildfires leave trail of destruction.** Firefighters worked to contain the Chelan fires in Chelan, Washington, which have burned over 155 square miles, forced about 1,500 residents to evacuate, and destroyed an estimated 50 homes August 14 – August 15. Officials announced that due to the volume of active wildfires burning in Idaho, Washington, and Oregon, 200 active-duty U.S. National Guard members were called in to assist with containment.
Source: http://www.komonews.com/news/local/Wash-wildfires-leave-path-of-destruction-National-Guard-called-up-322049361.html

21. *August 17, KOLO 8 Reno* – (California) **Walker Fire 3,770 acres and 10% contained.** Crew reached 10 percent containment August 17 of the 3,770-acre Walker Fire burning in Mono County, California. The fire prompted evacuations and the closure of the campgrounds in Lower Lee Vining Canyon.
Source: http://www.kolotv.com/home/headlines/Walker-Fire-2200-Acres-and-10-Contained-322051342.html

Emergency Services Sector

22. *August 16, WQAD 8 Moline* – (Illinois) **Illinois Department of Corrections inadvertently shares Social Security numbers of 1,000 employees.** State officials reported August 16 that the Illinois Department of Corrections discovered August 14 that the personal information, including Social Security numbers of over 1,000 department employees from its Lawrence and Dixon Correctional Centers was inadvertently shared in a Freedom of Information Act request. Officials are working to notify the individuals impacted.
Source: http://wqad.com/2015/08/16/illinois-department-of-corrections-inadvertently-shares-social-security-numbers-of-1000-employees/

Information Technology Sector

23. *August 18, Securityweek* – (International) **High severity flaw in Android allows arbitrary code execution.** Security researchers from Trend Micro discovered a heap overflow vulnerability in the Android operating system's (OS) mediaserver Audio Policy Service, AudioEffect component, in which an app requiring no permissions could be used to execute arbitrary code. The vulnerability was patched in August security updates.
Source: http://www.securityweek.com/high-severity-flaw-android-allows-arbitrary-code-execution

24. *August 18, Securityweek* – (International) **Darkode member admits selling access to spam botnet.** A New York member of the Darkode hacker forums pleaded guilty August 17 for his involvement in a scheme in which computers of Facebook users were infected with the Slenfbot worm and the "Facebook Spreader" malware, which used

victim account information to spread. The suspect and co-conspirators allegedly received $200 - $300 for every 10,000 active infections from 2011 – 2012.
Source: http://www.securityweek.com/darkode-member-admits-selling-access-spam-botnet

25. *August 18, Threatpost* – (International) **Reflection DDoS attacks abusing RPC Portmapper.** Officials from Level 3 Communications observed attackers utilizing Remote Procedure Call (RPC) Portmapper services for reflection distributed denial-of-service (DDoS) attacks between June and August, representing a new and effective method for bandwidth saturation.
Source: https://threatpost.com/reflection-ddos-attacks-abusing-rpc-portmapper/114318

For another story, see item **2**

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

26. *August 18, WTAE 4 Pittsburgh* – (Pennsylvania) **4-alarm fire destroys historic Washington County inn.** A 4-alarm fire August 18 at The Century Inn bed-and-breakfast in Scenery Hill, Pennsylvania, prompted 20 fire companies to remain on site for nearly 5 hours to contain the blaze, which left extensive damage. The building was safely evacuated and no guests were checked in during the fire.
Source: http://www.wtae.com/news/4alarm-fire-destroys-historic-washington-county-inn/34774604

27. *August 17, WATE 6 Knoxville* – (Tennessee) **24 displaced, 2 firefighters with minor injuries after East Knoxville apartment fire.** Twenty-four residents were displaced and 2 firefighters suffered minor injured following an August 17 fire at the Green Hills Apartments in Knoxville after the fire spread to the roof of the building and destroyed 4 apartment units. Fire crews extinguished the flames and an investigation is ongoing to determine the cause of the fire.
Source: http://wate.com/2015/08/17/knoxville-crews-battle-large-apartment-building-fire/

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.