Homeland Security

Daily Open Source Infrastructure Report
10 August 2015

Top Stories

- American Airlines Group Inc., is investigating a suspected hack into its system after Sabre Corp. confirmed a recent breach possibly tied to hackers who targeted United Airlines, American health insurers, and U.S. Government agencies. – *Bloomberg* (See item **10**)

- One million gallons of wastewater containing heavy metals from the Gold King Mine near Silverton, Colorado spilled into the Animas River after machinery damaged a plug August 5. – *Denver Post* (See item **16**)

- New York health officials issued an order August 6 for thousands of city buildings with water-cooling towers to assess and disinfect in response to a Legionnaire's outbreak that has killed 10 people and sickened at least 100 others. – *New York Times* (See item **18**)

- Check Point security researchers discovered Android vulnerabilities dubbed "Certifi-gate" affecting nearly all devices in which an attacker can gain unrestricted access, steal personal data, and track locations, among other actions. – *Help Net Security* (See item **29**)

Fast Jump Menu

PRODUCTION INDUSTRIES

- Energy
- Chemical
- Nuclear Reactors, Materials, and Waste
- Critical Manufacturing
- Defense Industrial Base
- Dams

SUSTENANCE and HEALTH

- Food and Agriculture
- Water and Wastewater Systems
- Healthcare and Public Health

SERVICE INDUSTRIES

- Financial Services
- Transportation Systems
- Information Technology
- Communications
- Commercial Facilities

FEDERAL and STATE

- Government Facilities
- Emergency Services

Energy Sector

1. *August 7, Infosecurity Magazine* – (International) **Trend Micro uncovers attacks on Internet-connected petrol stations.** Trend Micro experts investigating data attacks against automated gas tank systems using a custom international honeypot dubbed GasPot presented research at Black Hat 2015 which found 12 pump identifications, 4 pump modifications and 2 denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks against the systems from February – July 2015. Researchers suspect that several hacktivist groups, including the Iranian Dark Coders Team and the Syrian Electronic Army, were behind the attacks, a majority of which targeted the U.S.
   Source: http://www.infosecurity-magazine.com/news/trend-micro-uncovers-attacks-on/

2. *August 6, Alaska Dispatch News* – (Alaska) **Alaska oil and gas producer that took State tax credits faces fraud charges.** The U.S. Securities and Exchange Commission announced August 6 charges against Knoxville-based Miller Energy Resources that the company allegedly inflated values of oil and gas properties acquired in Cook Inlet in 2009 by over $400 million, leading to fraudulent financial reports regarding the company's net income and total assets. A former and current executive were also implicated in the civil claims filed August 6.
   Source: https://www.adn.com/article/20150806/alaska-oil-and-gas-producer-took-state-tax-credits-faces-accounting-fraud-charges

For another story, see item **33**

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

3. *August 6, Augusta Chronicle* – (Georgia) **Flammable chemical halts Defense Waste Processing Facility operations while safety reviewed.** Officials from Savannah River Remediation, the liquid waste contractor at the Defense Waste Processing Facility in Savannah, reported that operations that mix nuclear waste with molten glass into vitrified waste canisters are halted until October after crews discovered that an anti-foam chemical used in the process was flammable during an outage in April. The company anticipates no long-term impact to the production schedule.
   Source: http://chronicle.augusta.com/news/metro/2015-08-06/flammable-chemical-halts-defense-waste-processing-facility-operations-while

For another story, see item **33**

Critical Manufacturing Sector

4. *August 6, IDG News Service* – (International) **Tesla patches Model S after researchers hack car's software.** Tesla issued a security update to its Model S vehicle August 6 after security researchers from Lookout and CloudFlare were able to leverage

six flaws that allowed them to turn off the engine while it was in operation, change the speed and map information displayed on the vehicle's touch screen, open and close the trunk, and control the radio. The researchers reported that the hack required physical access to the vehicle.
Source: http://www.computerworld.com/article/2960802/security/tesla-patches-model-s-after-researchers-hack-cars-software.html#tk.rss_security

5. *August 6, Threatpost* – (International) **Gone in less than a second.** A security researcher unveiled a wallet-sized device, called Rolljam, that can be hidden underneath a vehicle and can intercept codes used to unlock most cars and garage doors employing rolling codes, by jamming the signal and replaying the next rolling code in the sequence. The developer previously created a device that was able to intercept communication between certain vehicles and the OnStar RemoteLink mobile application to locate, unlock, and remotely start a vehicle.
Source: https://threatpost.com/gone-in-less-than-a-second/114154

6. *August 6, U.S. Consumer Product Safety Commission* – (National) **Viking Range expands dishwasher recall due to fire hazard.** Viking Range LLC of Greenwood, Mississippi, issued an expanded recall August 6 of about 17,300 Viking Professional, Designer, and Custom Panel dishwashers manufactured before April 2011 due to an issue with an electrical component that could cause the unit to overheat, posing a fire hazard. The product was sold at specialty and retail stores nationwide from 2008 – 2012.
Source: http://www.cpsc.gov/en/Recalls/2015/Viking-Range-Expands-Dishwasher-Recall/

For additional stories, see items **1** and **33**

Defense Industrial Base Sector

7. *August 6, Stars and Stripes* – (International) **Unauthorized repairs sideline Navy's three newest fast-attack subs.** U.S. Navy officials reported August 5 that the USS John Warner, the USS Minnesota, and the USS North Dakota fast-attack submarines are to be held in port at the Yokosuka Naval Base in Japan due to concerns over pipe elbows used to send steam to the submarine turbines, after General Dynamics Electric Boat determined that three elbows supplied by a subcontractor required additional testing and repair due to unauthorized and undocumented weld repairs performed on the parts.
Source: http://www.military.com/daily-news/2015/08/06/unauthorized-repairs-sideline-navys-three-newest-subs.html

Financial Services Sector

8. *August 5, Delaware County Daily Times* – (Pennsylvania) **Glen Mills man pleads guilty to fraud, tax evasion.** The previous owner of the former Arcadia Capital Group, Inc., pleaded guilty August 5 to a scheme in which he and others allegedly solicited almost $10 million in real estate investments, the majority of which were diverted for

personal use or payments to prior investors.
Source: http://www.delcotimes.com/general-news/20150805/glen-mills-man-pleads-guilty-to-fraud-tax-evasion

9. *August 6, South Florida Sun-Sentinel* – (Florida) **Man accused of installing credit-card skimmers in Boca Raton, Delray Beach.** Authorities reported August 4 that a Delray Beach man was arrested for allegedly working with a partner to plant ATM skimming devices in at least 6 Publix store locations, stealing a total of $27,774 from over 25 people.
Source: http://www.sun-sentinel.com/local/palm-beach/delray-beach/fl-delray-beach-credit-card-skimmers-20150806-story.html

For another story, see item **2**

Transportation Systems Sector

10. *August 7, Bloomberg* – (International) **American Airlines, Sabre said to be hit in hacks backed by China.** American Airlines Group Inc., is investigating a suspected hack into its system after Sabre Corp., a clearinghouse for travel reservations which shares some network infrastructure with the airline, confirmed a recent breach possibly tied to the same China-linked hackers who targeted United Airlines, major American health insurers, and U.S. Government agencies. Sabre is unsure of the extent of the breach, but warns it may expose millions of flight records, hotel bookings, and car rentals.
Source: http://www.bloomberg.com/news/articles/2015-08-07/american-airlines-sabre-said-to-be-hit-in-hacks-backed-by-china

11. *August 7, NBC News* – (International) **United Airlines jet makes emergency landing after 'sparks' spotted in cabin.** United Airlines Flight UA935 from London to Los Angeles declared a midair emergency August 7 and returned to Heathrow Airport shortly after take-off when a mechanical issue caused sparks in several seats. No injuries were reported, and maintenance teams are inspecting the plane.
Source: http://www.nbcnews.com/business/travel/united-airlines-jet-makes-emergency-landing-over-mechanical-issue-n405831

12. *August 6, KCRA 3 Sacramento* – (California) **Highway 88 in Amador County closed due to big rig crash.** The California Highway Patrol warned motorists that Highway 88 in Amador County may remain closed until August 8 after a semi-truck carrying gasoline overturned near Buckhorn Ridge Road August 6, creating a HAZMAT situation.
Source: http://www.kcra.com/news/local-news/news-sierra/hwy-88-in-amador-county-closed-due-to-big-rig-crash/34573360

13. *August 6, Associated Press* – (New York) **Minor delays after smoke forces evacuation of LIRR train.** A smoldering track between the Penn Station and Forest Hills train stations in New York forced the evacuation of passengers and delayed service on the Long Island Rail Road August 6. No injuries were reported.

Source: http://www.washingtontimes.com/news/2015/aug/6/minor-delays-after-smoke-forces-evacuation-of-lirr/

Food and Agriculture Sector

14. *August 6, Denver Post* – (Colorado) **Virus hits Colorado livestock again this summer.** The Colorado Department of Agriculture and State veterinarians reported August 6 that horses, mules, and cattle at 53 locations in 8 counties were quarantined after testing positive for the presence of vesicular stomatitis, and that 14 locations previously under quarantine were recently released.
Source: http://www.denverpost.com/business/ci_28597523/virus-hits-colorado-livestock-again-this-summer

Water and Wastewater Systems Sector

15. *August 7, Ada News* – (Oklahoma) **Konawa residents directed to boil water before using.** A spokeswoman for the Oklahoma Department of Environmental Quality announced a boil advisory for the town of Konawa August 6 after an analysis of two of three water samples revealed E. coli.
Source: http://www.theadanews.com/news/konawa-residents-directed-to-boil-water-before-using/article_2ccccc8a-3d04-11e5-b5da-8bbb6b8db3b6.html

16. *August 6, Denver Post* – (Colorado) **Animas River fouled by 1 million gallons of contaminated mine water.** One million gallons of wastewater containing zinc, copper, iron and other heavy metals from the abandoned Gold King Mine near Silverton, Colorado entered the Animas River after heavy machinery from the U.S. Environmental Protection Agency damaged a plug August 5. The river was closed to recreational use while health and environmental officials evaluate the damage, and agricultural users were advised to shut off water intakes along the river.
Source: http://www.denverpost.com/environment/ci_28595759/animas-river-contaminated-by-1-million-gallons-contaminated

For another story, see item **18**

Healthcare and Public Health Sector

17. *August 6, KRON 4 San Francisco* – (California) **Patients at UCSF Medical Center possibly exposed to infection.** The chief medical officer at the University of California, San Francisco Medical Center stated August 6 that 471 patients may have been exposed to infection after the medical center did not properly clean cystoscopes used in several procedures between January and June. The medical center is offering patients free blood testing for Hepatitis B, C, and HIV.
Source: http://kron4.com/2015/08/06/only-on-4-patients-at-ucsf-medical-center-possibly-exposed-to-infection/

18. *August 6, New York Times* – (New York) **New York ordering tests of water-cooling towers amid Legionnaires' outbreak.** New York health officials issued an order

August 6 for thousands of buildings in the city with water-cooling towers to assess and disinfect units within the next 2 weeks in response to a Legionnaires' outbreak in the South Bronx that has killed 10 people and sickened at least 100 others. The mayor stated that building owners who did not comply with the order could face legal sanctions.
Source: http://www.nytimes.com/2015/08/07/nyregion/new-york-ordering-tests-of-water-cooling-towers-amid-legionnaires-outbreak.html

19. *August 5, U.S. Attorney's Office, District of Massachusetts* – (Massachusetts) **Clinical director of home care agency convicted of health care fraud scheme.** The clinical director of At Home VNA (AHVNA), a Waltham-based home health agency, was convicted August 5 for her role in a multi-million dollar Medicare fraud scheme where she and the agency's owner submitted over $27 million in fraudulent home health care claims and received more than $20 million from Medicare. A majority of the claims were medically unnecessary and employees were trained on how to convince senior citizens to enroll with AHVNA and falsify patients' assessments.
Source: https://www.fbi.gov/boston/press-releases/2015/clinical-director-of-home-care-agency-convicted-of-health-care-fraud-scheme

For another story, see item **33**

Government Facilities Sector

20. *August 6, Associated Press* – (California) **Residents return to devastation after massive California wildfire.** Crews reached 45 percent containment August 6 of the 69,600-acre Rocky Fire burning in northern California that destroyed 43 homes. About 800 people were allowed to return to Lake County while evacuation orders for surrounding areas remained.
Source: http://www.nbcnews.com/storyline/western-wildfires/residents-return-devastation-after-massive-california-wildfire-n405636

21. *August 6, KBZK 7 Bozeman* – (Montana) **Reynolds Creek Fire in Glacier National Park now 67% contained.** Crews reached 67 percent containment August 6 of the 3,913-acre Reynolds Creek Fire burning in Glacier National Park in Montana.
Source: http://www.kbzk.com/story/29730522/reynolds-creek-fire-in-glacier-national-park-now-67-contained

22. *August 6, Baker City Herald* – (Oregon) **Lime Hill fire at 12,000 acres, notice of possible evacuation canceled for Huntington.** Potential evacuation orders for the city of Huntington in Baker County were cancelled August 6 after authorities determined that the 12,000-acre Lime Hill Fire was no longer a threat to the community. Fire crews continued work to contain the fire.
Source: http://www.bakercityherald.com/Local-News/Lime-Hill-fire-at-12000-acres-notice-of-possible-evacuation-canceled

23. *August 6, WAFF 48 Huntsville* – (Tennessee) **4 children taken to hospital after Lincoln Co. school bus wreck.** Four students were injured when a school bus carrying

Unity School and Lincoln High School students overturned on Hickory Ridge Road in Lincoln County, Tennessee, August 4.
Source: http://www.waff.com/story/29723845/2-children-taken-to-hospital-after-lincoln-co-school-bus-wreck

24. *August 6, Los Angeles Times* – (California) **Child contracts plague while visiting Yosemite National Park.** The California Department of Public Health announced August 6 that it will conduct an environmental evaluation in the Stanislaus National Forest, Yosemite National Park, and surrounding areas after a child contracted the plague in July following a camping trip at Crane Flat Campground in Yosemite National Park. Signs were posted at campgrounds around the park providing visitors with information on how to prevent plague exposure.
Source: http://www.msn.com/en-us/news/us/child-contracts-plague-while-visiting-yosemite-national-park/ar-BBlsJK9

For another story, see item **33**

Emergency Services Sector

Nothing to report

Information Technology Sector

25. *August 7, Securityweek* – (International) **Mozilla patches Firefox zero-day exploited in the wild.** Mozilla released Firefox version 39.0.3 to address a zero-day vulnerability in the browser's mechanism that enforces JavaScript's same origin policy and Firefox's PDF Viewer, in which an attacker can inject a JavaScript payload to steal local files containing sensitive information. The attack was observed being exploited in the wild, targeting certain types of files hosted on Windows and Linux systems.
Source: http://www.securityweek.com/mozilla-patches-firefox-zero-day-exploited-wild

26. *August 6, Help Net Security* – (International) **Zero-day disclosure-to-weaponization period cut in half.** Security researchers from Malwarebytes reported a trending decrease in time between the disclosure and weaponization of zero-day vulnerabilities, evident in a 50 percent drop in average weaponization times in the last 10 months, citing the fallout from the Hacking Team breach as a contributing factor.
Source: http://www.net-security.org/secworld.php?id=18727

27. *August 6, IDG News Service* – (International) **Attackers could use Internet route hijacking to get fraudulent HTTPS certificates.** Security researchers at Black Hat 2015 highlighted the threats posed by Border Gateway Protocol (BGP) hijacking attacks, also known as route leaking, in which an attacker could tailor attacks to specific geographic regions by tricking a certificate authority (CA) into issuing a valid certificate for a domain name that they do not own.
Source: http://www.computerworld.com/article/2959542/security/attackers-could-use-internet-route-hijacking-to-get-fraudulent-https-certificates.html#tk.rss_security

28. *August 6, Softpedia* – (International) **80 vulnerabilities found in iOS in 2015, 10 in Android.** Secunia released findings from a report on security vulnerability trends for the first 7 months of 2015 revealing an increase of "extremely critical" and "highly critical" threats, a trending increase in zero-day exploits, and a total of 80 reported vulnerabilities in Apple's iOS operating system (OS) versus 10 in Android devices. Researchers cited Apple's control of its OS and patch cycle as the cause for higher number if iOS vulnerabilities.
Source: http://news.softpedia.com/news/80-vulnerabilities-found-in-ios-in-2015-10-in-android-488676.shtml

29. *August 6, Help Net Security* – (International) **Easily exploitable Certifi-gate bug opens Android devices to hijacking.** Security researchers from Check Point's mobile security research team discovered a set of vulnerabilities in the Android operating system (OS) dubbed "Certifi-gate" in the architecture of mobile Remote Support Tools (mRSTs) used by almost every Android device manufacturer in which an attacker can leverage hash collisions, inter-process communication (IPC) abuse, and certificate forging to gain unrestricted device access and steal personal data, track locations, and turn on microphones, among other actions.
Source: http://www.net-security.org/secworld.php?id=18730

30. *August 6, IDG News Service* – (International) **Design flaw in Intel processors opens door to rootkits, researcher says.** A security researcher from the Battelle Memorial Institute disclosed a vulnerability in the x86 processor architecture in which an attacker could install a rootkit in the processor's System Management Mode (SMM), enabling destructive actions such as wiping the Unified Extensible Firmware Interface (UEFI) or re-infecting the operating system (OS) after a fresh install.
Source: http://www.networkworld.com/article/2965873/design-flaw-in-intel-processors-opens-door-to-rootkits-researcher-says.html#tk.rss_all

31. *August 6, Threatpost* – (International) **Updated DGA Changer malware generates fake domain stream.** Researchers from Seculert published findings from a report revealing that the DGA Changer downloader malware now has the capability to generate a stream of fake domains once it determines that it is being run in a virtual environment, the first reported instance of malware generating fake domain generation algorithms (DGA).
Source: https://threatpost.com/updated-dga-changer-malware-generates-fake-domain-stream/114159

32. *August 6, SC Magazine* – (International) **DDoS attacks rage on, primarily impacting U.S. and Chinese entities.** Kaspersky Lab released findings from its DDoS Intelligence Report Q2 2015, revealing that 77 percent of the distributed denial-of-service (DDoS) attacks from April to June impacted 10 countries, primarily the U.S. and China. The report recorded the longest attack at 205 hours, and the peak number at 1,960 May 7, attributing their popularity to the ease in which the attacks can be arranged.
Source: http://www.scmagazine.com/kaspersky-lab-releases-q2-ddos-

report/article/431034/

33. *August 6, Threatpost* – (International) **BLEKey device breaks RFID physical access controls.** Researchers at Black Hat 2015 released details from a number of proof of concept attacks highlighting the weaknesses in the Wiegand protocol used in radio-frequency identification (RFID) readers and other proximity card devices, which they were able exploit by using a device dubbed BLEKey to read cleartext data sent from card readers to door controllers to clone cards or send data to a mobile application that can unlock doors remotely at any time.
Source: https://threatpost.com/blekey-device-breaks-rfid-physical-access-controls/114163

For additional stories, see items **1**, **4**, **5**, and **10**

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 items **28** and **29**

Commercial Facilities Sector

34. *August 6, Troy Messenger* – (Alabama) **Storm collapses roof at Walmart, damages shopping center.** Shoppers were evacuated after the roof of a Walmart in Troy, Alabama, partially collapsed August 6 due to an apparent tornado. Two other nearby businesses suffered damage and debris was scattered throughout parking lots and surrounding buildings.
Source: http://www.troymessenger.com/2015/08/06/storm-collapses-roof-at-walmart/

35. *August 6, WGHP 8 High Point* – (North Carolina) **North Carolina Zoo to be closed Friday due to storm damage.** Damage from an August 6 storm prompted the closure of the North Carolina Zoo August 7 after several trees were knocked down, posing a hazard for visitors.
Source: http://myfox8.com/2015/08/06/north-carolina-zoo-to-be-closed-friday-due-to-storm-damage/

36. *August 6, South Jersey Times* – (New Jersey) **Deptford Mall reopened after water main break.** The Deptford Mall in New Jersey was closed for approximately 3 hours August 6 following a water main break that flooded part of the mall parking lot. Repairs were made and the mall reopened under its regular business hours.
Source: http://www.nj.com/gloucester-county/index.ssf/2015/08/deptford_mall_reopened_after_water_main_break.html

37. *August 6, KRWG 22 Las Cruces* – (New Mexico) **Suspicious package at Mesilla Valley Mall deemed no further threat to public, LCPD investigating.** Patrons were evacuated and the Mesilla Valley Mall was closed for 5 hours August 6 after a suspicious package was found inside the mall. Officers removed the package and deemed it safe once it was determined to be of no threat to the public.
Source: http://krwg.org/post/suspicous-package-mesilla-valley-mall-deemed-no-further-threat-public-lcpd-investigating

For additional stories, see items **9**, **10**, **18**, and **33**

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.