



Daily Open Source Infrastructure Report 13 July 2015

Top Stories

- General Motors announced a recall July 10 of about 690,000 model year 2007 – 2012 Saturn, GMC, and Buick SUVs in the U.S. due to an issue with gas struts that could cause lift gates to close unexpectedly. – *CNBC* (See item [3](#))
- Federal officials announced July 9 that the recent breach of the U.S. Office of Personnel Management’s computer systems affected roughly 21.5 million people, up from previous estimates of 4.2 million. – *CNN* (See item [19](#))
- The alleged mastermind of an Estonian-based international cyber fraud group pleaded guilty to his role in operation “Ghost Click”, in which he and co-conspirators installed the DNSChanger trojan on 4 million computers in over 100 countries and collected \$14 million through clickjacking and ad fraud. – *Securityweek* (See item [24](#))
- Service Systems Associates reported point-of-sale malware installed on its credit and debit card processing systems may have compromised payment information of zoo gift shop customers in over 12 cities nationwide. – *Krebs on Security* (See item [28](#))

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. *July 10, Associated Press* – (Louisiana) **New Orleans accepts \$45 million from BP in oil spill settlement.** The city of New Orleans accepted \$45 million from BP July 9 as part of an \$18.7 billion settlement between the oil company and 5 states as compensation for damages stemming from the 2010 Deepwater Horizon oil spill in the Gulf of Mexico.
Source: <http://fuelfix.com/blog/2015/07/10/new-orleans-accepts-45-million-from-bp-in-oil-spill-settlement/#33996101=0>

Chemical Industry Sector

2. *July 9, Houston Chronicle* – (Texas) **OSHA labels DuPont a severe violator after four killed in Texas.** The U.S. Department of Labor's Occupational Health and Safety Administration added \$273,000 in penalties against DuPont for additional violations July 9 after proposing a fine of \$99,000 in May for violations related to the fatalities and failures that led to a leak of 23,000 pounds of toxic methyl mercaptan at its La Porte, Texas plant last November.
Source: <http://www.chron.com/news/houston-texas/article/OSHA-labels-DuPont-a-severe-violator-after-four-6375592.php>

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

3. *July 10, CNBC* – (National) **General Motors recalling nearly 780K crossover SUVs.** General Motors announced a recall July 10 of about 690,000 model year 2007 – 2012 Saturn Outlook, GMC Acadia, Chevrolet Traverse, and Buick Enclave vehicles in the U.S. due to an issue with gas struts in which dirt may cause them to prematurely wear, causing the power lift gate to close unexpectedly. Fifty-six injuries have been reported in connection with the issue.
Source: <http://www.cnbc.com/2015/07/10/general-motors-recalling-nearly-780k-crossover-suvs.html>
4. *July 9, U.S. Department of Labor* – (Illinois) **Auto parts manufacturer ignores safety hazards, worker loses fingertip.** The Occupational Safety and Health Administration cited Carol Stream-based FIC America Corp., July 9 for one repeated, nine serious, and one other-than-serious safety violation for failing to use safety procedures and locking devices to prevent machines from operating during service and maintenance, among other violations. Proposed penalties total \$89,000.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=28242

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *July 9, KCRA 3 Sacramento* – (California) **‘Dropout Bandit’ sought in 3 NorCal bank robberies.** The FBI is searching for a suspect dubbed the ‘Dropout Bandit’ who allegedly robbed at least 3 Schools Credit Union branches in Sacramento since March. Source: <http://www.kcra.com/news/local-news/news-sacramento/dropout-bandit-sought-in-3-norcal-bank-robberies/34076724>
6. *July 9, WXIX 19 Cincinnati* – (Ohio; Kentucky; Indiana) **‘Sock Hat Bandit’ indicted for bank robberies during two month period.** A Dayton man dubbed the “Sock Hat Bandit” was indicted July 9 for three robberies at the Hebron U.S. Bank, Bellevue Fifth Third Bank, and Independence Fifth Third Bank in Kentucky between May – June, while authorities continue to investigate his role in at least six more robberies across Ohio and Indiana in the two-month span. Source: <http://www.fox19.com/story/29514988/sock-hat-bandit-indicted-for-bank-robberies-in-two-month-period>
7. *July 9, Dow Jones Business News* – (National) **Adviser, racer convicted in fraud case.** A former financial adviser and a retired professional race car driver were convicted July 9 of stealing over \$30 million from investors over 10 years by falsely promising investments, including land development in Hawaii and a credit card company in Arizona, and that the men used holding companies to divert funds for personal expenses. Source: <http://www.nasdaq.com/article/adviser-racer-convicted-in-fraud-case-20150709-01084>

Transportation Systems Sector

8. *July 10, KXAS 5 Dallas-Fort Worth* – (Texas) **Interstate 45 shut down after Dallas officer crashes into stalled car.** Interstate 45 in Dallas was shut down for several hours July 10 while crews cleared the scene of an accident involving a police car that crashed into a stalled vehicle. No injuries were reported. Source: <http://www.nbcdfw.com/news/local/I-45-Shut-Down-After-Dallas-Officer-Crashes-into-Stalled-Car-313187981.html>
9. *July 10, WOWK 13 Charleston* – (West Virginia) **I-64 in Huntington back open after deadly crash.** Interstate 64 East in Huntington was shut down for over 5 hours July 10 while crews responded to an accident that injured 2 police officers and killed 1 person after a driver rear-ended a police cruiser. Source: <http://www.wowktv.com/story/29517561/deadly-crash-shuts-down-i-64-east-in-huntington>
10. *July 10, Associated Press* – (Nevada) **DMV camera, scanner systems back up after electrical problem.** A Las Vegas Department of Motor Vehicles location was evacuated and camera and scanner systems used for identification cards and driver’s

licenses were down State-wide July 9 following a transformer blow-out near the East Sahara facility.

Source:

<http://www.dailyjournal.net/view/story/2650f6022d794bbbb970a4bff2490fb/NV--DMV-Outage>

11. *July 9, WBBM 2 Chicago* – (Illinois) **Flight to Boston evacuated after engine catches fire during takeoff at Midway.** Passengers on a Southwest Airlines flight from Chicago to Boston were evacuated off the plane July 8 after an engine caught fire during takeoff, prompting an emergency landing at Midway International Airport. No injuries were reported.

Source: <http://chicago.cbslocal.com/2015/07/09/flight-to-boston-evacuated-after-engine-catches-fire-during-takeoff-at-midway/>

For another story, see item [20](#)

Food and Agriculture Sector

12. *July 10, Food Safety News* – (Minnesota) **Federal, State officials investigating Minnesota Salmonella outbreaks.** The U.S. Centers for Disease Control and Prevention, U.S. Department of Agriculture, and Minnesota Departments of Health and Agriculture officials are reportedly investigating two outbreaks of Salmonella Enteritidis linked to Barber Foods brand and Antioch Farms brand chicken products that infected 7 people between April – June.

Source: http://www.foodsafetynews.com/2015/07/cdc-fsis-minnesota-officials-investigating-two-salmonella-outbreaks-linked-to-raw-frozen-chicken-entrees/#.VZ_PU_1VhBc

13. *July 9, Associated Press* – (Arkansas) **Little Rock man accused of defrauding USDA feeding program.** The U.S. Attorney’s office announced charges July 9 against a Little Rock man accused of allegedly defrauding a U.S. Department of Agriculture community feeding program by overstating how many children were served at “Our Children of Tomorrow,” an organization he sponsored.

Source: <http://www.katv.com/story/29513720/little-rock-man-accused-of-defrauding-usda-feeding-program>

14. *July 8, U.S. Department of Agriculture* – (California) **Bassett and Walker International, Inc., recall beef products produced without benefit of import inspection.** Toronto, Canada-based Bassett & Walker International, Inc., issued a recall July 7 for about 1,540 pounds of beef lip products from Australia after the Food Safety and Inspection Service found that the items were not inspected at the port of entry. The products were distributed to retail outlets and restaurants in the San Diego area.

Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-098-2015-release>

Water and Wastewater Systems Sector

15. *July 9, KTXS 20 Sweetwater* – (Texas) **Wastewater spilled in Snyder, public water safe.** The city of Snyder Water Reclamation Plant reported that an estimated 50,000 gallons of wastewater spilled near Deep Creek July 7 after a line in the facility collapsed due to heavy rainfall. Crews cleaned the site of the spill after plugging the line and diverting the flow.
Source: <http://www.ktxs.com/news/wastewater-spilled-in-snyder-residents-encouraged-to-boil-water1/34085072>
16. *July 9, WQAD 8 Moline* – (Illinois) **Thousands of gallons of untreated wastewater discharged in Clinton.** Thousands of gallons of untreated wastewater went into the Mississippi River after a repair failed in a force main in Clinton, Iowa, causing about 2,000 gallons per minute to spill July 8.
Source: <http://wqad.com/2015/07/09/thousands-of-gallons-of-untreated-wastewater-discharged-in-clinton/>

For another story, see item [20](#)

Healthcare and Public Health Sector

17. *July 10, Lorain County Chronicle-Telegram* – (Ohio) **Elyria hospital patients' records improperly accessed by worker.** A University Hospital Elyria Medical Center official announced July 9 a security breach affecting 300 patients after a former employee allegedly accessed sensitive information using the hospital's electronic medical record system outside of normal duties. The hospital said there is no evidence the information was misused and notifications were sent to affected patients beginning July 2.
Source: <http://chronicle.northcoastnow.com/2015/07/10/elyria-hospital-patients-records-improperly-accessed-worker/>
18. *July 9, Reuters* – (New York) **Walgreen to pay \$22.4 million in N.Y. Medicaid improper billing case.** A \$22.4 million settlement between Walgreen Co., and the New York attorney general was revealed July 9 after allegations that Trinity Healthcare LLC, primarily owned by Walgreen Co, submitted false claims to the government for Synagis, an injectable respiratory drug for premature infants.
Source: <http://www.businessinsider.com/r-walgreen-to-pay-224-million-in-ny-medicaid-improper-billing-case-2015-7>

Government Facilities Sector

19. *July 10, CNN* – (National) **OPM government data breach impacted 21.5 million.** Federal officials announced July 9 that the June breach of the U.S. Office of Personnel Management's computer systems affected roughly 21.5 million people, up from the 4.2 million estimate originally announced, including security clearance application information from 19.7 million applicants and information regarding 1.8 million non-applicants comprised of spouses and partners.
Source: <http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/index.html>

20. *July 9, WPRI 12 Providence* – (Rhode Island) **DMV reopens after power outage.** Officials are investigating the cause of a power outage which left the Division of Motor Vehicles and the Department of Labor and Training offices in Cranston, Rhode Island without water or power for several hours July 8, suspending operations for the two agencies until July 9.
Source: <http://wpri.com/2015/07/09/dmv-reopens-after-power-outage/>

Emergency Services Sector

21. *July 9, Washington Post* – (Virginia) **Ex-Loudon sheriff's deputy charged with stealing asset forfeiture money.** A former Loudon County sheriff's deputy was charged July 10 with allegedly embezzling more than \$200,000 from the office's asset-forfeiture program over a span of 3 years.
Source: http://www.washingtonpost.com/local/crime/ex-loudoun-sheriffs-deputy-accused-of-stealing-asset-forfeiture-money/2015/07/09/c8c69e3c-24c6-11e5-b72c-2b7d516e1e0e_story.html

For another story, see item [9](#)

Information Technology Sector

22. *July 10, Securityweek* – (International) **Chinese APT group uses Hacking Team's Flash Player exploit.** Security researchers from Volexity reported that the Wekby advanced persistent threat group (APT), also known as APT 18, Dynamite Panda, and TG-0416, was leveraging an Adobe Flash Player exploit revealed through the July breach of the software company Hacking Team by sending spear-phishing emails purporting to be from Adobe which directed users to download a compromised Flash Player file containing malware.
Source: <http://www.securityweek.com/chinese-apt-group-uses-hacking-team%E2%80%99s-flash-player-exploit>
23. *July 10, Help Net Security* – (International) **VMware fixes host privilege escalation bug in Workstation, Player, Horizon View.** VMware issued patches addressing a privilege escalation vulnerability in the company's Workstation, Player, and Horizon View Client for Microsoft Windows in which an attacker could leverage a lack of a discretionary access control list (DACL) in a process to elevate privileges and execute code.
Source: <http://www.net-security.org/secworld.php?id=18613>
24. *July 9, Securityweek* – (International) **Estonian man pleads guilty to role in DNSChanger botnet scheme.** The alleged mastermind of an Estonian-based international cyber fraud group pleaded guilty to his role in a 2007 – 2011 operation dubbed "Ghost Click" in which he and co-conspirators installed the DNSChanger trojan on 4 million computers in over 100 countries and collected over \$14 million through clickjacking and ad fraud via the malware.
Source: <http://www.securityweek.com/estonian-man-pleads-guilty-role-dnschanger->

[botnet-scheme](#)

25. *July 9, IDG News Service* – (International) **Hacking Team claims terrorists can now use its tools.** The Italian security company Hacking Team warned July 8 that the release of 400 gigabytes (GB) of internal data in a July 5 breach of its systems represented an “extremely dangerous” situation and that terrorists and other threat actors could potentially leverage available code to deploy software against any target. Source: http://www.computerworld.com/article/2946093/security0/hacking-team-claims-terrorists-can-now-use-its-tools.html#tk.rss_security

For another story, see item [28](#)

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 9, U.S. Federal Communications Commission* – (National) **TerraCom, YourTel to pay \$3.5M to resolve consumer privacy violations.** The U.S. Federal Communications Commission’s Enforcement Bureau entered into a \$3.5 million settlement with Terracom Inc., and YourTel America, to resolve violations after an investigation revealed the companies failed to properly protect confidentiality of personal information they received from more than 300,000 consumers. Source: <https://www.fcc.gov/document/terra-com-yourtel-pay-35m-resolve-consumer-privacy-violations>

Commercial Facilities Sector

27. *July 9, Cecil Whig* – (Maryland) **Electrical fire damages Port Deposit restaurant/bar.** Officials reported that an electrical malfunction is to blame for a fire that caused an estimated \$10,000 in structural damage inside of a Port Deposit restaurant and bar July 9. Source: http://www.cecildaily.com/news/local_news/article_eaa9bc6-d993-5b24-b18d-73fd5c6f61b4.html
28. *July 9, Krebs on Security* – (National) **Credit card breach at a zoo near you.** Denver-based Service Systems Associates reported that malware installed on point-of-sale (PoS) credit and debit card processing systems at zoo gifts shops in at least 12 cities nationwide may have compromised the payment information of customers who used the systems between March 23 – June 25. Source: <https://krebsonsecurity.com/2015/07/credit-card-breach-at-a-zoo-near-you/>

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

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.