



Daily Open Source Infrastructure Report 09 July 2015

Top Stories

- U.S. Federal Trade Commission officials announced July 7 that \$54 million in settlements with 14 companies owned by 2 Johnson County, Missouri men will resolve charges that the men allegedly used personal information to take out loans without permission, among other charges. – *Kansas City Star* (See item [5](#))
- The Federal Aviation Administration reported July 8 that about 3,500 United Airlines flights were grounded and delayed nationwide throughout major airports after its computer system experienced a network connectivity issue. – *NBC News* (See item [7](#))
- Amtrak train headed to St. Louis from Chicago was delayed 9 hours total after a semi-truck accident in Joliet, Illinois initially delayed the train and a derailment in Dwight, Illinois caused a consecutive delay July 6. – *Associated Press* (See item [8](#))
- Symantec reported that a cybercriminal group dubbed Morpho that was known for hacking Apple, Microsoft, Facebook, and Twitter, has extended its cyber-espionage to hit research-and-development related computer systems. – *Dark Reading* (See item [16](#))

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 8, WPMI 15 Mobile; WBMA 58 Birmingham* – (Alabama) **4 injured in tanker explosion in Alabama.** First responders closed 4 miles of County Road 11 in Pelham, Alabama and evacuated nearby homes for at least 7 hours after an accident involving a semi-truck injured 4 and spilled 9,000 gallons of fuel, sparking a fire.
Source: http://www.utv44.com/shared/news/features/top-stories/stories/wpmi_4-injured-tanker-explosion-alabama-21801.shtml#.VZ07KvIVhBc
2. *July 8, Reuters* – (North Dakota) **Power outage in North Dakota’s capital delays drilling rig data.** A power outage at a substation operated by MDU Resources Group in Bismarck, North Dakota July 8 disabled computer servers that provide data on output statistics for the state’s daily drilling rig count. The rig count is monitored by the state’s Department of Mineral Resources and delivers guidance on future oil production for nearly 15,000 wells.
Source: <http://af.reuters.com/article/commoditiesNews/idAFL1N0ZO0VR20150708>

For another story, see item [16](#)

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

For additional stories, see items [16](#) and [17](#)

Defense Industrial Base Sector

3. *July 8, Naval Open Source Intelligence* – (South Carolina) **Fighter jet, plane collide in deadly midair collision.** A U.S. National Transportation Safety Board official reported July 8 that a U.S. Air Force F-16 fighter jet collided midair with a small Cessna plane July 7 over South Carolina, killing the Cessna’s occupants. The F-16 pilot was taken to Shaw Air Force Base for observation and an investigation is ongoing to determine the cause of the collision.
Source: <http://nosint.blogspot.com/2015/07/fighter-jet-plane-collide-in-deadly.html>

Financial Services Sector

4. *July 8, South Florida Sun-Sentinel* – (Florida) **FBI hunts suspected serial bank robber dubbed ‘Filter Bandit’.** The FBI announced a \$5,000 reward for information leading to the arrest of a suspect dubbed the “Filter Bandit,” who allegedly stole over \$60,000 from 7 banks in Broward County since August 2014, ending with the robbery

of a BB&T Bank June 16 in Davie.

Source: <http://www.sun-sentinel.com/local/broward/fl-filter-bandit-bank-robber-20150707-story.html>

5. *July 7, Kansas City Star* – (Missouri) **Firms accused of faking loans, draining bank accounts settle with Feds.** U.S. Federal Trade Commission officials announced \$54 million in settlements July 7 with 14 companies owned by 2 Johnson County, Missouri men to resolve charges that the men allegedly used personal data from short-term payday loan Web sites in conjunction with “lead generators” to take out loans for people without their permission, and that they produced phony loan documentation, misstated loan terms, and misrepresented the transactions to banks.
Source: <http://www.kansascity.com/news/government-politics/article26662321.html>
6. *July 7, WKBW 7 Buffalo* – (New York) **Bank vice president stole \$5.3M in scheme.** A former M&T Bank vice president from Williamsville, New York pleaded guilty July 7 to a \$5.3 million loan scheme in which he created at least 12 “funding loans” in the name of credit-worthy entities, which he then distributed to customers of his choosing.
Source: <http://www.wkbw.com/news/police-blotter/bank-vice-president-stole-53m-in-scheme>

Transportation Systems Sector

7. *June 8, NBC News* – (National) **United Airlines flights no longer grounded, delays remain.** The Federal Aviation Administration reported July 8 that about 3,500 United Airlines flights were grounded and delayed nationwide throughout major airports after its computer system experienced a network connectivity issue. Crews were able to repair the computer system, but delays can affect up to 373 flights.
Source: <http://www.nbcnews.com/business/travel/united-airlines-passengers-say-flights-grounded-nationwide-n388536>
8. *July 7, Associated Press* – (Illinois) **Freight train derailment causes ordeal for Amtrak passengers.** Amtrak train headed to St. Louis from Chicago was delayed 9 hours total after a semi-truck accident in Joliet, Illinois initially delayed the train and a derailment in Dwight, Illinois caused a consecutive delay July 6. The train arrived to its destination 14 hours after leaving Chicago.
Source: <http://fox2now.com/2015/07/07/freight-train-derailment-causes-ordeal-for-amtrak-passengers/>
9. *July 7, KTBS 3 Shreveport* – (Louisiana) **Train collides with 18-wheeler in Caddo Parish.** Highway 1 in both directions in Caddo Parish was shut down until further notice July 7 while crews investigate an accident that involved a semi-truck and a train that caused a fire. There were no reports of injuries.
Source: <http://www.ktbs.com/story/29496994/train-collides-with-18-wheeler-in-caddo-parish>
10. *July 7, KNBC 4 Los Angeles* – (California) **Fire shuts down lanes on 5 Freeway in Commerce.** A fire shut down 5 Freeway in Commerce for over 6 hours July 7 while

crews assessed the damage on the roadway and the structural integrity of the bridge.
Source: <http://www.nbclosangeles.com/news/local/Fire-Shuts-Down-5-Freeway-Commerce-311990661.html>

For additional stories, see items [1](#) and [3](#)

Food and Agriculture Sector

11. *July 7, Associated Press* – (North Carolina) **North Carolina salmonella outbreak kills 1, sickens nearly 250.** The North Carolina Department of Health and Human Services reported July 7 that 248 cases of illnesses and 1 death were associated with the Lexington restaurant, Tarheel Q after testing showed salmonella contamination. Tarheel Q faces several lawsuits, and reopened its doors July 1.
Source: <http://www.insurancejournal.com/news/southeast/2015/07/07/374209.htm>

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

For additional stories, see items [16](#) and [19](#)

Government Facilities Sector

For another story, see item [19](#)

Emergency Services Sector

12. *July 8, KNTV 11 San Jose; Associated Press* – (California) **Gun used in pier 14 shooting belonged to Federal agent: sources.** San Francisco authorities reported July 7 that the gun used in a July 1 shooting that led to the death of a woman was allegedly stolen from a Federal agent's vehicle. Further investigations are ongoing to determine how the shooter obtained the weapon.
Source: <http://www.nbcbayarea.com/news/local/Francisco-Sanchez-Pier-14-Heroin-Deportation-Immigration-Debate-Steinle-312139981.html?988888>
13. *July 7, Associated Press* – (Louisiana) **La. officer arrested for obstruction of justice.** New Orleans police authorities arrested one of its police officers July 6 on charges for obstruction of justice, malfeasance in office, and theft after a June investigation revealed the officer had failed to process evidence after arresting a culprit.
Source: <http://www.policeone.com/officer-misconduct-internal-affairs/articles/8652245-La-officer-arrested-for-obstruction-of-justice>
14. *July 7, Associated Press* – (South Carolina) **New charges in SC church shooting: attempted murder.** South Carolina authorities reported July 7 that the June 17 shooter charged with killing 9 people while attending Bible Study at Emanuel African

Methodist Episcopal Church, is being charged on 3 new counts of attempted murder after leaving 3 survivors from the shooting.

Source: <http://www.policeone.com/mass-casualty/articles/8652388-New-charges-in-SC-church-shooting-Attempted-murder>

15. *July 7, Associated Press* – (Delaware) **Security chief at Delaware women’s prison charged with having sex with inmate.** Delaware State police arrested and charged the superintendent at the Baylor Women’s Correctional Institution in New Castle, Delaware for allegedly having sexual relations with an inmate June 12.

Source:

<http://www.tribtown.com/view/story/91afd6232045421a821d161cf087fb08/DE--Prison-Official-Suspended>

Information Technology Sector

16. *July 8, Dark Reading* – (International) **Cybercriminal group spying on U.S., European businesses for profit.** Symantec reported that a cybercriminal group dubbed Morpho that was known for hacking Apple, Microsoft, Facebook, and Twitter, has extended its cyber-espionage to hit research-and-development related computer systems in 49 different multi-billion dollar pharmaceutical, software, Internet, oil, and metal mining commodities organizations across 20 countries, with the majority being in the U.S. Researchers believe the group has U.S. ties and is run by an organized crime ring.

Source: <http://www.darkreading.com/endpoint/cybercriminal-group-spying-on-us-european-businesses-for-profit/d/d-id/1321221>

17. *July 8, Securityweek* – (International) **Hacker search engine becomes the new Internet of Things search engine.** The developer of the Shodan Internet device search engine reported that the search engine exposes the systemic vulnerabilities present in consumer-grade Internet of Things hubs due to a poor security posture, where many hubs still use default passwords and have telnet enabled. Once compromised attackers could leverage hubs to monitor sensor data or determine if someone is home.

Source: <http://www.securityweek.com/hacker-search-engine-becomes-new-internet-things-search-engine>

18. *July 8, Securityweek* – (International) **Adobe patches Hacking Team’s Flash Player zero-day.** Adobe released an emergency update for its Flash Player to address a zero-day vulnerability in the ActionScript 3 ByteArray class, which could allow a remote, unauthenticated attacker to execute arbitrary code. The vulnerability was exposed after hackers breached and dumped corporate information of the Hacking Team surveillance software company.

Source: <http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day>

19. *July 7, Securityweek* – (International) **ANTlabs patches vulnerabilities in gateway products.** ANTLabs released patches for several of its gateway products addressing a Structured Query Language (SQL) injection flaw in the default login page in which a

remote attacker could execute arbitrary queries, and a cross-site scripting (XSS) vulnerability in the admin login page that could allow an attacker to obtain login credentials from the administrator panel.

Source: <http://www.securityweek.com/antlabs-patches-vulnerabilities-gateway-products>

20. *July 7, Securityweek* – (International) **Zero-day exploits leaked in Hacking Team breach.** Security researchers from Trend Micro and Symantec reported that data from a recently confirmed Hacking Team breach contained several zero-day vulnerabilities and exploits, including a use-after-free (UAF) flaw affecting Adobe Flash Player versions 9 and later on Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari, and a Microsoft Windows kernel vulnerability.
Source: <http://www.securityweek.com/zero-day-exploits-leaked-hacking-team-breach>

21. *July 7, Network World* – (International) **Microsoft security tool fails malware detection test.** AV Test released results from a recent experiment revealing that Microsoft Security Essentials performed the worst out of 11 tested antivirus products, only detecting 87 percent of malware in real-time tests, when the others were all at least 95 percent effective.
Source: http://www.networkworld.com/article/2944810/microsoft-subnet/microsoft-windows-security-tool-fails-malware-detection-test.html#tk.rss_all

22. *July 7, Threatpost* – (International) **Crypto leaders: “exceptional access” will undo security.** Cryptography experts released a report warning of the long term economic and security risks associated with “exceptional access,” a U.S. government initiative to maintain access to cryptographic keys to secure information over the Internet primarily for law enforcement use.
Source: <https://threatpost.com/crypto-leaders-exceptional-access-will-undo-security/113639>

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

For additional stories, see items [16](#) and [19](#)

Commercial Facilities Sector

23. *July 7, KCBS 2 Los Angeles* – (California) **1 killed, 4 others injured in a 2-car crash into Gardena Donut King.** A 2-car collision at Donut King II in Gardena, California injured 4 people and killed 1 other July 7, after both vehicles entered an intersection

simultaneously and crashed into the shop. The donut shop was open at the time of the crash but no customers were injured.

Source: <http://losangeles.cbslocal.com/2015/07/07/5-injured-1-critical-in-2-car-crash-into-gardena-donut-king/>

24. *July 7, KSBY 6 San Luis Obispo* – (California) **Mustang Village Apartments evacuated after bomb threat.** Residents and employees at the Mustang Village Apartments in San Luis Obispo, California were evacuated for 2 hours after the San Luis Obispo Police Department received a bomb threat July 7. Police found no threats to the building and are investigating the incident.
Source: <http://www.ksby.com/story/29494558/mustang-village-apartments-evacuated-after-threat>

25. *July 7, KCBS 2 Los Angeles* – (California) **Crews knock down fire that engulfed church near Glendale Freeway.** A July 7 bush fire caused extensive damage to the Church of Jesus Christ of Latter-day Saints in Glendale, California and prompted about 185 firefighters and several water-dropping helicopters to remain on site for over 2 hours to contain the incident. No injuries were reported and the cause of the bush fire is under investigation.
Source: <http://losangeles.cbslocal.com/2015/07/07/brush-fire-threatens-church-near-glendale-freeway/>

For another story, see item [19](#)

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.