Homeland Security

Daily Open Source Infrastructure Report 16 July 2015

Top Stories

- Over 168,000 Duke Energy customers in Ohio and Kentucky were without power July 14 and 7,000 remained without service after recent storms July 15. – *WXIX 19 Cincinnati* (See item **2**)
- Three suspects pleaded guilty in Florida July 14 to their roles in a $64 million fraud scheme in which Great Country Mortgage Bankers employees targeted customers with U.S. Federal Housing Administration loans.– *WFOR 4 Miami; Associated Press* (See item **10**)
- A July 14 report revealed that the U.S. Office of Personnel Management has yet to officially notify 21.5 million victims of a cyberattack discovered in May. – *Reuters* (See item **22**)
- Officials filed charges against 12 suspects affiliated with the Darkode hacker Web forum after officials shut down the site and arrested or searched 70 members worldwide. – *IDG News Service* (See item **25**)

Fast Jump Menu

Energy Sector

1. *July 15, Huntsville Times –* (Alabama) **Storms rip through the Birmingham metro area, damage and power outages reported.** A line of thunderstorms across Alabama left 35,500 in the metro Birmingham area and an additional 23,700 in other regions across the state without power July 14. The Alabama Department of Transportation also reported that all lanes of Interstate 59 northbound near mile marker 139 was shut down due to a downed tree after the storms.
   Source: http://www.al.com/news/birmingham/index.ssf/2015/07/storms_rip_through_birmingham.html

2. *July 15, WXIX 19 Cincinnati* – (Ohio; Kentucky) **Duke energy: outages should be restored by Thursday night.** Over 168,000 Duke Energy customers in Ohio and Northern Kentucky were without power July 14 after powerful storms damaged power lines across the area, and 7,000 remained without service July 15. Duke Energy officials expect power to be restored to customers by July 16.
   Source: http://www.fox19.com/story/29550788/thousands-without-power-following-storms

3. *July 15, WCHS 8 Charleston* – (West Virginia) **About 22,000 without power on Wednesday following severe storms.** About 22,000 West Virginia residents were without power July 15 after severe storms knocked out service to almost 30,000 customers. American Electric Power reported that service in some areas could take until July 17 to restore, and Appalachian Power crews were working across the State to repair damage.
   Source: http://www.wchstv.com/news/features/eyewitness-news/stories/About-30-000-Still-Without-Power-On-Wednesday-Following-Severe-Storms-167278.shtml#.VaZZqflViko

4. *July 14, Associated Press* – (California) **U.S. agency faulted for inaction after Santa Barbara oil spill.** The U.S. House of Representatives Energy and Power Subcommittee faulted the Pipeline and Hazardous Materials Safety Administration in a statement July 14 for failing to complete over a dozen Federal requirements enacted in 2011 in response to a May oil spill on the California coast caused by a heavily corroded section of pipe.
   Source: http://www.sfgate.com/nation/article/U-S-agency-faulted-for-inaction-after-Santa-6384579.php

Chemical Industry Sector

5. *July 14, Michigan Live* – (Michigan) **HAZMAT situation at Haviland Enterprises 'under control'.** A hazardous materials chemical leak at Haviland Enterprises in Grand Rapids, Michigan prompted a large emergency response after "mostly oxygen" was released from a packaging line where multiple chemicals were blended. HAZMAT crews cleaned the site and no injuries were reported.
   Source: http://www.mlive.com/news/grand-

rapids/index.ssf/2015/07/hazmat_situation_at_haviland_e_1.html

Nuclear Reactors, Materials, and Waste Sector

6. *July 15, Associated Press* – (Virginia) **Nuclear power plant reactors shut down for repairs.** Two nuclear reactors at Dominion Virginia Power's Surry County plant were shut down July 11—13 for a planned maintenance on one of the units' coolant pumps and minor repairs to a second unit's spray valve attached to its coolant system.
   Source: http://wavy.com/2015/07/15/nuclear-power-plant-reactors-shut-down-for-repairs/

Critical Manufacturing Sector

7. *July 15, Reuters* – (National) **Toyota recalls 625,000 hybrid cars globally for software glitch.** Toyota Motor Corp., announced a recall July 15 for about 120,000 hybrid Prius vehicles in the U.S. due to a software glitch that could shut down that vehicle's hybrid system while in operation. The recall affects models produced between May 2010 and November 2014.
   Source: http://www.reuters.com/article/2015/07/15/us-toyota-recall-idUSKCN0PP0EF20150715

8. *July 15, KHQ 6 Spokane* – (Washington) **Five injured in explosion at aerospace plant in Newport, Wash.** Residences and businesses within 2,000 feet of the Zodiac Aerospace Plant in Newport, Washington were evacuated after a July 14 explosion in the plant caused a floor to collapse, injuring 5 workers and prompting a HAZMAT response. Authorities are investigating the cause of the incident.
   Source: http://www.khq.com/story/29550076/explosion-reported-at-aerospace-plant-in-newport-wash

Defense Industrial Base Sector

9. *July 14, Army Times* – (National) **Current, former Guard members warned of data breach.** An Army National Guard spokesperson announced July 14 a recent security breach affecting over 850,000 current and former Guard members was caused by a mishandled data transfer, not a cyberattack.
   Source: http://www.armytimes.com/story/military/guard-reserve/2015/07/14/national-guard-data-breach-opm-ssn/30150319/

Financial Services Sector

10. *July 14, WFOR 4 Miami; Associated Press* – (Florida) **Three plead guilty in $64M mortgage fraud scheme.** Three suspects pleaded guilty July 14 to their roles in a $64 million mortgage fraud scheme in which Great Country Mortgage Bankers employees targeted first-time, low-income, and poor-credit buyers with U.S. Federal Housing Administration loans which they would obtain with falsified documents, before selling them at a profit. Twenty-five have pleaded guilty in connection with the scheme.
    Source: http://miami.cbslocal.com/2015/07/14/three-plead-guilty-in-64m-mortgage-

fraud-scheme/

11. *July 14, U.S. Securities and Exchange Commission* – (National) **SEC Charges 34 defendants in microcap market manipulation schemes.** The U.S. Securities and Exchange Commission charged 15 individuals and 19 entities July 14 for allegedly attempting to manipulate the trading of microcap stocks by acting as unregistered broker-dealers for customers wanting to hide their stock ownership and manipulate the microcap market.
Source: http://www.sec.gov/news/pressrelease/2015-146.html

Transportation Systems Sector

12. *June 15, WDAY 6 Fargo* – (Montana) **Train derailment damages miles of track near Wolf Point, Montana.** Crews are working overnight after a BNSF train hauling liquefied petroleum gas, hydrocarbon and alcohol derailed and destroyed 3 to 4 tracks near Wolf Point July 14. The derailment delayed Amtrak service and it remains unknown when service will be resumed and no injuries or hazardous material were spilled.
Source: http://www.wdaz.com/news/3797613-train-derailment-damages-miles-track-near-wolfpoint-montana

13. *July 14, ARLNow.com* – (Virginia) **Pantless man causes bomb scare on Lee Highway.** Lee Highway in Arlington was shut down for nearly 2 hours July 13 while police responded to a report of a man walking down the road with his pants around his ankles while threatening he had a bomb. No bomb was found and the roadway reopened shortly after.
Source: http://www.arlnow.com/2015/07/14/pantless-man-causes-bomb-scare-on-lee-highway/

14. *July 14, WVEC 13 Hamptons Road* – (Virginia) **I-64 reopened after accident and fuel leak at HRBT.** The Hampton Roads Bridge-Tunnel in Norfolk was closed to eastbound traffic July 14 for approximately 2 hours after a 2-vehicle accident on Interstate 64 caused fuel to leak onto the roadway. No injuries were reported.
Source: http://www.13newsnow.com/story/traffic/2015/07/14/i-64-shutdown-at-the-hrbt-for-accident-and-fuel-leak/30141117/

15. *July 14, WJBK 2 Detroit* – (Michigan) **Dangling semi truck driver rescued on I-94 overpass.** Interstate 94 in Romulus was shut down for nearly 3 hours July 14 while crews responded to an accident that left a semi-truck dangling off an overpass causing the driver to be trapped in the cab for over an hour. The cause of the accident remains under investigation and the driver was uninjured.
Source: http://www.myfoxdetroit.com/story/29546450/dangling-semi-shuts-down-part-of-i-94

For another story, see item **1**

Food and Agriculture Sector

16. *July 14, U.S. Food and Drug Administration* – (Washington) **Homemade recalls pickles and sauces because of possible health risk.** Homemade, a Leavenworth, Washington establishment is recalling pickle and sauce products due to high levels of pH found in samples that can grow Clostridium botulinum July 14. The products were packaged in clear glass bottles with metal caps and shipped to retailers and fruit stands in Washington State.
Source: http://www.fda.gov/Safety/Recalls/ucm454846.htm

17. *July 14, Food Safety News* – (National) **Omaha Steaks recalls stuffed chicken breast products for Salmonella.** Omaha Steaks of Omaha, Nebraska is recalling stuffed chicken breast products manufactured by Barber Foods due to potential Salmonella contamination. The products were shipped nationwide.
Source: http://www.foodsafetynews.com/2015/07/omaha-steaks-recalls-stuffed-chicken-breast-products-for-salmonella-risk/#.VaZONflVhBc

Water and Wastewater Systems Sector

18. *July 14, Washington Post* – (Washington, D.C.) **E. coli found in creek in Northwest Washington, area closed to public.** D.C. Water officials closed Soapstone Creek to the public July 14 while investigating elevated levels of E.coli in the creek that was found after a leak in an 18-inch sanitary sewer pipe spilled sewage into the creek.
Source: http://www.washingtonpost.com/news/local/wp/2015/07/14/e-coli-found-in-creek-in-northwest-washington-area-closed-to-public/

19. *July 14, WLNS 36 Lansing* – (Michigan) **Sewage spill in St. Joseph River leads to health advisory.** Hillsdale city officials are advising residents to avoid contact with the St. Joseph River after nearly 70,000 gallons of untreated sewage and waste water spilled into the river due to a recent power outage at the plant July 14. Crews have stopped the spill and are taking steps to correct the electrical problem.
Source: http://wlns.com/2015/07/14/massive-sewage-spill-in-st-joseph-river-leads-to-health-advisory/

Healthcare and Public Health Sector

20. *July 15, Pittsburgh Post-Gazette* – (Pennsylvania) **Misdirected email faulted in data breach affecting hundreds of UPMC insurance customers.** An email meant for a physician’s office in Lawrence County was mistakenly sent to an incorrect address, revealing sensitive personal information for 722 UPMC Health Plan members, the insurance company announced July 15. The breach was discovered June 4, and the Department of Health and Human Services was alerted July 2.
Source: http://www.post-gazette.com/business/healthcare-business/2015/07/15/Misdirected-email-compromises-hundreds-of-UPMC-insurance-customers/stories/201507150176

21. *July 14, WKYC 3 Cleveland* – (Ohio) **Canton VA outpatient clinic closed after man**

douses self with gas. The outpatient clinic at Louis Stokes Cleveland VA Medical Center in Canton, Ohio was closed July 14 after a man entered the facility and doused himself with gasoline before being intercepted by a security guard in a failed attempt to set himself and the building on fire. The clinic remained closed after the scene was cleared due to a lingering odor, and reopened July 15.
Source: http://www.wkyc.com/story/news/local/canton/2015/07/14/canton-va-outpatient-clinic-closed-after-man-douses-himself-with-gas/30137631/

Government Facilities Sector

22. *July 15, Reuters* – (National) **OPM hack: U.S. has not notified 21.5 million victims of massive data breach.** A July 14 report revealed that the U.S. Office of Personnel Management (OPM) has yet to officially notify 21.5 million victims of a cyberattack discovered in May which exposed sensitive information disclosed in security clearance investigations. Multiple Federal agencies are working with OPM to develop a central system to inform victims, although officials reported this could be delayed for several weeks due to the complicated nature of the data.
Source: http://www.ibtimes.com/opm-hack-us-has-not-notified-215-million-victims-massive-data-breach-2008940

23. *July 13, Springfield Republican* – (Massachusetts) **Adams man charged in ISIS plot – due in Springfield Federal court.** The U.S. Attorney's Office in Boston unsealed charges July 13 against a suspect who allegedly purchased weapons and planned terrorist attacks inspired by the Islamic State, including setting off improvised explosive devices in heavily populated areas such as college cafeterias.
Source:
http://www.masslive.com/news/index.ssf/2015/07/alexander_ciccolo_aka_ali_al_amriki_adams_isis_springfield_federal_court.html

Emergency Services Sector

24. *July 14, WESH 2 Orlando* – (Florida) **Weapons, equipment stolen from deputy's cruiser.** Thousands of dollars' worth of Florida's Orange County Sheriff's Office equipment, including a machine gun, a stun gun, riot gear, handcuffs, and a tactical vest, were stolen from an unmarked police cruiser July 12. An investigation is ongoing to find the culprit.
Source: http://www.wesh.com/news/weapons-equipment-stolen-from-deputys-cruiser/34159122

Information Technology Sector

25. *July 15, IDG News Service* – (International) **Darkode computer hacking forum shuts after investigation spanning 20 countries.** U.S. authorities filed hacking charges against 12 suspects affiliated with the Darkode hacker Web forum after the FBI and law enforcement organizations from 20 countries shut down the site and arrested or searched 70 Darkode members worldwide. The Web site allowed hackers to share technology and tradecraft used to infect computers and wireless devices of victims.

Source: http://www.networkworld.com/article/2948634/darkode-computer-hacking-forum-shuts-after-investigation-spanning-20-countries.html#tk.rss_all

26. *July 15, Softpedia* – (International) **Hacking Team malware hides in UEFI BIOS to survive PC reinstalls.** Security researchers from Trend Micro discovered that Hacking Team ensured surveillance malware persistence on systems by using Unified Extensible Firmware Interface (UEFI) Basic Input/Output System (BIOS) rootkit to re-install the malware every time it was deleted from the system.
Source: http://news.softpedia.com/news/hacking-team-malware-hides-in-bios-to-survive-pc-reinstalls-486949.shtml

27. *July 15, Securityweek* – (International) **Oracle patches Java zero-day, 192 other security bugs.** Oracle released updates addressing 193 security issues across multiple product lines, including a Java remote code execution vulnerability that was exploited by the advanced persistent threat (APT) group Pawn Storm, 54 flaws in third-party components in Oracle product distributions, and 23 vulnerabilities in Java SE that can be exploited remotely by an unauthenticated attacker, among other fixes.
Source: http://www.securityweek.com/oracle-patches-java-zero-day-192-other-security-bugs

28. *July 15, Help Net Security* – (International) **TeslaCrypt 2.0 makes it impossible to decrypt affected files.** Security researchers at Kaspersky Lab discovered that recent TeslaCrypt version 2.0 ransomware infections display a Cryptowall 3.0 Web page, possibly in an attempt to convince victims that the malware uses more robust encryption than it actually does.
Source: http://www.net-security.org/malware_news.php?id=3075

29. *July 15, Softpedia* – (International) **HTML5 can be used to hide malware in drive-by download attacks.** Italian security researchers discovered that Hypertext Markup Language 5 (HTML5)-based obfuscation techniques could be used to hide malware in drive-by download exploits using HTML technologies and application program interfaces (API).
Source: http://news.softpedia.com/news/html5-can-be-used-to-hide-malware-in-drive-by-download-attacks-486974.shtml

30. *July 14, Securityweek* – (International) **Microsoft patches Hacking Team zero-days, other vulnerabilities.** Microsoft released 14 bulletins addressing vulnerabilities in Windows, Office, SQL Server, and Internet Explorer, including a zero-day Jscript 9 use-after-free memory corruption bug in Internet Explorer 11 and a memory corruption flaw in the Adobe Type Manager Font Driver that could both allow an attacker to take complete control of a vulnerable system, as well as a remote code execution flaw affecting the Remote Desktop Protocol (RDP).
Source: http://www.securityweek.com/microsoft-patches-hacking-team-zero-days-other-vulnerabilities

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

31. *July 15, KTVT 11 Fort Worth* – (Texas) **Garland Apartment Building destroyed by fire.** A 2-alarm fire at the Forest Glen Apartments in Garland, Texas displaced 30 people after beginning inside a first-floor unit and spread to surround units July 15. Fire crews extinguished the flames and an investigation is ongoing to determine the cause of the incident.
Source: http://dfw.cbslocal.com/2015/07/15/garland-apartment-building-destroyed-by-fire/

32. *July 15, Jacksonville Florida Times-Union* – (Florida) **11 forced from Jacksonville apartments after early morning fire Wednesday damages units.** The Westgate apartments in Jacksonville, Florida sustained extensive damage after a July 15 fire destroyed 4 units and displaced 11 residents after beginning in a central apartment unit. Damages total over $100,000
Source: http://jacksonville.com/news/crime/2015-07-15/story/11-forced-jacksonville-apartments-after-early-morning-fire-wednesday

For another story, see item **8**

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.