



Daily Open Source Infrastructure Report 25 March 2016

Top Stories

- A severe storm prompted the cancellation of hundreds of flights and the closure of the Denver International Airport in Colorado for more than 6 hours March 23 – March 24. – *Fort Collins Coloradoan* (See item [11](#))
- A wildfire burned more than 400,000 acres in Kansas and Oklahoma March 24 and prompted the closure of U.S. 160 in Barber County for several hours March 23. – *KAKE 10 Wichita* (See item [18](#))
- Researchers reported that an advanced data-stealing universal serial bus (USB) trojan dubbed, “USB Thief” was found in the wild and can compromise a system by injecting itself into the execution chain of portable versions of popular applications and disguising itself as a plugin or a Dynamic Link Library (DLL) file. – *SecurityWeek* (See item [21](#))
- An additional 48 bikers were indicted March 23 for allegedly engaging in organized criminal activity following a May 2015 shootout between 2 rival motorcycle clubs at a restaurant in Waco, Texas, that killed 9 people. – *CNN* (See item [25](#))

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. *March 23, U.S. Environmental Protection Agency* – (West Virginia) **EPA settles with natural gas company for oil spill in Ohio River Tributary in Marshall Co., W. Va.** The U.S. Environmental Protection Agency reached a settlement with Williams Ohio Valley Midstream March 23 resolving an alleged violation of the Federal Clean Air Act following the discharge of approximately 132 barrels of natural gas condensate into a waterway after a 4-inch pipe ruptured at the company's facility in Moundsville, West Virginia. The company agreed to pay a \$14,440 penalty.
Source: <https://yosemite.epa.gov/opa/admpress.nsf/0/3a14de1961f1dc8185257f7f0056f890>
2. *March 23, Denver Post* – (Colorado) **Xcel Energy outages leave 290,000 Denver-area customers without power.** Xcel Energy crews worked March 24 to restore power to about 51,500 customers in the Denver area that remained without service after a March 23 storm dumped several inches of snow on power lines and knocked out service to approximately 290,000 customers.
Source: http://www.denverpost.com/news/ci_29674905/xcel-energy-power-outages-affecting-55-000-customers

Chemical Industry Sector

3. *March 23, WWL 4 New Orleans* – (Louisiana) **Tanker truck spills acid in Gentilly.** The New Orleans Fire Department reported March 23 that a tanker truck hauling methacrylic acid overturned in Gentilly, spilling about 9,000 gallons of the highly corrosive chemical. Officials plugged all area drains to stop the chemical from entering the waterways.
Source: <http://www.wwltv.com/news/local/orleans/tanker-truck-spills-acid-in-no-east/98681653>
4. *March 23, WTAW 1620 AM College Station* – (Texas) **Chlorine leak prompts evacuation at College Station Middle School.** The College Station Middle School in Texas was evacuated March 23 after about 1,000 gallons of chlorine liquid, with a 10 percent concentration, leaked from a delivery truck and spilled into an area detention pond. HAZMAT crews cleaned the area and deemed the school safe.
Source: <http://wtaw.com/2016/03/23/chlorine-leak-prompts-evacuation-college-station-middle-school/>

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

5. *March 23, U.S. Department of Justice* – (International) **Chinese national pleads guilty to conspiring to hack into U.S. defense contractors' systems to steal sensitive military information.** The U.S. Department of Justice announced that a Chinese national pleaded guilty March 23 to participating with two others in China in a conspiracy to hack into computer networks of major U.S. defense contractors in order to steal military technical data. The businessman provided two co-conspirators with guidance regarding what persons, companies, and technologies to target, as well as which files and folders to steal once the individuals had successfully breached information technology systems.
Source: <https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive>

Financial Services Sector

6. *March 24, KTVU 2 Oakland* – (California) **Woman captures video of 'Bearded Bandit' arrest.** The FBI arrested a man dubbed the "Bearded Bandit" in Brentwood, California, March 23, after he allegedly committed 15 bank robberies that totaled \$28,000 in theft from the San Francisco Bay Area.
Source: <http://www.ktvu.com/news/112910236-story>
7. *March 23, Los Angeles Times* – (California) **'Bad Breath Bandit' strikes again at northern California bank, police say.** Authorities are searching for a man dubbed the "Bad Breath Bandit" who is suspected of robbing the El Dorado Savings Bank in Georgetown, California, March 21 at gunpoint. Officials stated that the man is tied to four other bank robberies in northern California in 2014.
Source: <http://www.latimes.com/local/lanow/la-me-ln-bad-breath-bandit-strikes-again-20160323-story.html>
8. *March 23, Forum of Fargo-Moorhead* – (North Dakota; Maryland) **Valley City State prof faces ID theft charges after police seize 200 credit cards.** A Chinese citizen working as an assistant professor at Valley City State University in North Dakota and Johns Hopkins University in Maryland was arrested March 22 after authorities discovered over 200 credit and gift cards, computers, electronic storage devices, and suspected counterfeit merchandise, among other items, in the professor's apartment and office. The investigation began after authorities received anonymous photographs revealing the large number of credit cards bearing different names in the suspect's apartment.
Source: <http://www.inforum.com/news/3993426-valley-city-state-prof-faces-id-theft-charges-after-police-seize-200-credit-cards>
9. *March 23, U.S. Department of Justice* – (International) **Miami businessman pleads guilty to foreign bribery and fraud charges in connection with Venezuela bribery scheme.** The owner of multiple U.S.-based energy companies pleaded guilty March 22 to foreign bribery and Federal fraud charges after he and a co-conspirator participated in a scheme to illicitly secure energy contracts from Venezuela's state-owned energy

company, Petroleos de Venezuela S.A. (PDVSA) by paying bribes and other things of value to PDVSA officials in order to win lucrative energy contracts, ensure spots on PDVSA approved vendor lists, and be given payment priority ahead of other vendors from 2009 – 2015. Officials stated that four other individuals pleaded guilty for their participation in the scheme.

Source: <https://www.justice.gov/opa/pr/miami-businessman-pleads-guilty-foreign-bribery-and-fraud-charges-connection-venezuela>

10. *March 23, Reuters* – (New Jersey) **FBI seeks help nabbing bank robber known as ‘Count Down Bandit’**. The FBI is searching March 23 for a man dubbed the “Count Down Bandit” who is suspected of committing at least seven robberies at banks around northern New Jersey, with his most recent taking place March 8. The suspect has reportedly targeted Hudson City bank branches.

Source: <http://www.reuters.com/article/us-new-jersey-bandit-idUSKCN0WP2PV>

Transportation Systems Sector

11. *March 24, Fort Collins Coloradoan* – (Colorado) **Transfort, DIA up and running, U.S. 287 and I-25 reopened**. A severe storm that dumped several inches of snow in Colorado prompted the cancellation of hundreds of flights and the closure of the Denver International Airport for more than 6 hours March 23 – March 24. Schools and universities as well as interstates and highways were also closed.

Source: <http://www.coloradoan.com/story/news/2016/03/23/snow-delays-start-psd-school-i25-north-closed/82141896/>

12. *March 24, Fox News; Associated Press* – (California; New York) **Flight attendant arrested after fleeing LAX, leaving cocaine and shoes behind**. A JetBlue flight attendant surrendered to U.S. Drug Enforcement Administration agents at John F. Kennedy International Airport in New York March 23 after she allegedly fled from Los Angeles International Airport March 18 when Transportation Security Administration agents discovered nearly 70 pounds of cocaine worth an estimated \$3 million in street value in her bags during a security screening.

Source: <http://www.foxnews.com/us/2016/03/24/flight-attendant-arrested-after-fleeing-lax-leaving-cocaine-and-shoes-behind.html>

For additional stories, see items [3](#), [18](#), and [20](#)

Food and Agriculture Sector

13. *March 24, U.S. Food and Drug Administration* – (National) **Gerber is voluntarily recalling two batches of Gerber Organic 2nd Foods Pouches due to a packaging defect that may result in product spoilage**. Gerber Products Company issued a voluntary recall March 24 for two variations of its Gerber Organic 2nd Foods Pouches products sold in 3.5-ounce packages due to a packaging defect that may result in product spoilage during transport and handling. The products were distributed to retailers nationwide and sold via the Internet.

Source: <http://www.fda.gov/Safety/Recalls/ucm492260.htm>

14. *March 24, U.S. Food and Drug Administration* – (New York; New Jersey) **AA USA Trading Inc. issues allergy alert on undeclared sulfites in AA Brand dried Ginger Slice.** AA USA Trading Inc., issued a recall March 23 for its dried Ginger Slice products sold in 8-ounce plastic bags due to misbranding and undeclared sulfites due to a breakdown in the packaging and labeling process. The products were distributed to retail stores in New York and New Jersey.
Source: <http://www.fda.gov/Safety/Recalls/ucm492252.htm>
15. *March 23, U.S. Department of Labor* – (Ohio) **Kroger butcher loses fingertip in unguarded band saw.** The Occupational Safety and Health Administration cited The Kroger Company with one repeat and one serious safety violation March 17 after an employee's finger was amputated by a band saw used to butcher meat, prompting an investigation at the Cincinnati, Ohio facility which revealed that the company had inadequate guards on machinery and that it lacked an energy isolation program. Proposed penalties total \$45,500.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=30528
16. *March 23, WBZ 4 Boston* – (Massachusetts) **Worker killed in Seaport District ammonia leak.** The Boston Fire Department and HAZMAT crews responded to a level 3 HAZMAT incident at the Stavis Seafoods warehouse in Boston March 23 due to an ammonia leak, which killed one employee and prompted the evacuation of four others. The leak was stopped after firefighters shut down the main valve and authorities were investigating the incident.
Source: <http://boston.cbslocal.com/2016/03/23/boston-firefighters-ammonia-leak-hazmat/>

Water and Wastewater Systems Sector

17. *March 24, MLive.com* – (Michigan) **60,000 gallons of raw sewage discharged near Jackson County Airport.** A blockage of grease in a 15-inch gravity sewer below Interstate 94 in Blackman Township led to a discharge of an estimated 60,000 gallons of raw sewage from March 20 – March 22, which impacted the Hurd Marvin Drain and Grand River. The waterways were treated with lime and an investigation is ongoing.
Source:
http://www.mlive.com/news/jackson/index.ssf/2016/03/60000_gallons_of_raw_sewage_di.html

Healthcare and Public Health Sector

See item [18](#)

Government Facilities Sector

18. *March 24, KAKE 10 Wichita* – (Kansas; Oklahoma) **Wildfire burns more than**

400,000 acres in Kansas, Oklahoma. The governor of Kansas declared a state of emergency March 24 due to a wildfire that burned more than 400,000 acres in Kansas and Oklahoma and prompted the closure of U.S. 160 in Barber County for several hours March 23. Medicine Lodge Hospital was evacuated while fire crews worked to contain the blaze which continued to threaten 800 – 1,000 homes and businesses.

Source: <http://www.kake.com/home/headlines/Mile-wide-grass-fire-in-Comanche-County-373205531.html>

19. *March 23, Associated Press* – (Ohio) **Ohio man charged with threats to harm U.S. President, presidential candidate.** A Cleveland man was charged March 23 for calling the U.S. Secret Service February 28 and threatening to kill the U.S. President and a cause bodily harm to a presidential candidate.
Source: <http://www.timesleaderonline.com/page/content.detail/id/1128031/Ohio-man-charged-with-threats-to-harm-Obama--Hillary-Clinton.html?isap=1&nav=5019>
20. *March 23, BigIslandNow.com* – (Hawaii) **West Hawai'i brush fire burns 1,300 acres.** Crews worked March 23 to contain a brush fire that burned about 1,300 acres in West Hawaii and prompted the closure of Highway 190. Authorities believe that the fire was ignited by a lightning strike.
Source: <http://bigislandnow.com/2016/03/23/west-hawaii-brush-fire-closes-highway-190/>

For additional stories, see items [4](#), [5](#), [8](#), and [11](#)

Emergency Services Sector

Nothing to report

Information Technology Sector

21. *March 23, SecurityWeek* – (International) **Sophisticated USB trojan spotted in the wild.** Researchers from ESET reported that an advanced data-stealing universal serial bus (USB) trojan dubbed, “USB Thief” was found in the wild and can compromise a system by injecting itself into the execution chain of portable versions of popular applications and disguising itself as a plugin or a Dynamic Link Library (DLL) file. The threat is bound to a single USB drive and was reported to have four executables and two configuration files that enable it to avoid detection and prevent researchers from detecting, copying, and analyzing the malware.
Source: <http://www.securityweek.com/sophisticated-usb-trojan-spotted-wild>
22. *March 24, Help Net Security* – (International) **OS X zero day bug allows hackers to bypass system integrity protection.** A security researcher discovered a non-memory corruption flaw in Apple Inc.,’s operating system (OS) X that could allow an attacker to compromise OS X and iOS systems by executing arbitrary code on any binary and escalating attackers’ privileges to root and/or bypass Apple’s System Integrity Protection feature. Researchers stated the zero-day vulnerability was not exploited by attackers, but the flaw could potentially be used in highly targeted or State sponsored

attacks.

Source: <https://www.helpnetsecurity.com/2016/03/24/os-x-zero-day-bug-allows-hackers-bypass-system-integrity-protection/>

23. *March 24, SecurityWeek* – (International) **Oracle reissues patch for two-year-old Java.** Oracle Corporation released updates for two of its Java SE products addressing a sandbox escape flaw after researchers discovered the previously patched flaw could be bypassed to allow a remote, unauthenticated attacker trick users into visiting a malicious Web site. The new update successfully patches the flaw within Java SE 8 Update 77 and Java SE 7 Update 99.

Source: <http://www.securityweek.com/oracle-reissues-patch-two-year-old-java-flaw>

For additional stories, see items [5](#) and [24](#)

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

24. *March 24, Help Net Security* – (International) **RCE flaw affects DVRs sold by over 70 different vendors.** A security researcher from RSA Security discovered a remote code execution (RCE) flaw in digital video recorders (DVRs) sold by more than 70 different vendors and manufactured by a Chinese company, TVT Digital Technology Co., Ltd., can allow an attacker to gain root access to the DVR as the vulnerability resides within the implementation of the Hypertext Transfer Protocol (HTTP) server included in the firmware. The implementation opens ports 81/82 of the device to the Internet, which is included in over 30,000 devices internationally.

Source: <https://www.helpnetsecurity.com/2016/03/24/rce-flaw-dvrs-70-vendors/>

Commercial Facilities Sector

25. *March 24, CNN* – (Texas) **48 more bikers indicted in deadly shootout at Waco, Texas, restaurant.** The McLennan County Criminal District Attorney announced March 23 that an additional 48 bikers were indicted for allegedly engaging in organized criminal activity following a May 2015 shootout between 2 rival motorcycle clubs at the Twin Peaks restaurant in Waco, Texas, that killed 9 people. The total number of indictments increased to more than 150 people.

Source: <http://www.cnn.com/2016/03/24/us/waco-more-bikers-indicted/>

26. *March 23, San Diego Union-Tribune* – (California) **Fire engulfs Kearny mesa foam business.** A March 23 fire at a San Diego building housing several businesses caused about \$850,000 in damages to E-Z Flow Foam Systems after the blaze accidentally began in the warehouse following a malfunction during routine equipment testing. The

incident was contained and HAZMAT crews were deployed to ensure burned debris were not toxic.

Source: <http://www.sandiegouniontribune.com/news/2016/mar/23/fire-foam-systems-kearny-mesa/>

27. *March 23, San Diego Union-Tribune* – (California) **Fire, smoke damages El Cajon dollar store.** The J's Dollar Store in El Cajon, California, sustained about \$175,000 in damages due to a March 22 fire. The incident was contained and no injuries were reported.

Source: <http://www.sandiegouniontribune.com/news/2016/mar/23/el-cajon-dollar-store-fire/>

28. *March 23, Burbank Beat* – (Illinois) **Police believe liquor store fire was intentionally set.** Authorities are investigating a March 21 fire as arson after the blaze destroyed Oak Park Liquor & Tobacco in Burbank, Illinois. Officials stated the fire began at the front of the store, burned through the ceiling, and spread to the rest of the building.

Source: <http://www.burbankbeat.net/news/police-believe-liquor-store-fire-was-intentionally-set>

For another story, see item [18](#)

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.