Daily Open Source Infrastructure Report
09 April 2015

Top Stories

- An April 7 power surge temporarily knocked out electricity to a number of Federal government buildings, museums, several Metro stations, restaurants, offices, and residences in Washington, D.C. and Maryland. – *Washington Post* (See item **1**)
- All seven passengers were killed when an aircraft crashed about 2 miles from the Central Illinois Regional Airport in Bloomington April 7. – *Associated Press* (See item **7**)
- Fidelis reported that hackers have co-opted the AlienSpy remote access tool (RAT) and are spreading it via phishing messages to deliver the Citadel banking trojan and establish backdoors inside a number of critical infrastructure operations. – *Threatpost* (See item **22**)
- A report released by Trend Micro and the Organization of the American States revealed that in the last year 40 percent of 575 security leaders throughout critical infrastructure sectors had dealt with network shutdown attempts and 60 percent had faced hacking attempts aimed at stealing vital information, among other findings. – *Securityweek* (See item **24**)

Fast Jump Menu

Energy Sector

1. *April 7, Washington Post* – (Washington, D.C.; Maryland) **Power surge knocks out electrical service in parts of D.C. region.** An April 7 power surge that occurred when a Pepco transmission conductor in Mechanicsville, Maryland, broke free and fell to the ground, temporarily knocked out electricity to the White House, U.S. Department of State, U.S. Department of Justice, a number of other government buildings, museums, several Metro stations, restaurants, offices, and residences in Washington, D.C., and prompted the closure of the University of Maryland at College Park campus.
Source: http://www.washingtonpost.com/local/scattered-power-outages-reported-across-dc-area/2015/04/07/8f4e8b84-dd49-11e4-a500-1c5bb1d8ff6a_story.html

2. *April 7, Associated Press* – (Montana) **Broken pipeline that spilled into Yellowstone to be removed.** Bridger Pipeline LLC announced April 7 that it will attempt to remove a broken section of its breached pipeline April 8 and send it to a laboratory for metallurgical analysis while regulators continue to investigate the cause of a January 30,000-gallon oil spill into Montana's Yellowstone River that contaminated downstream water supplies for thousands of people in Glendive.
Source: http://www.seattlepi.com/business/energy/article/Pipeline-that-spilled-into-Yellowstone-to-be-6183881.php

For additional stories, see items **22** and **24**

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

See items **3** and **24**

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

3. *April 7, Warwick Post* – (Rhode Island) **Troopers arrest Warwick man for embezzling $142K from manufacturer.** Rhode Island State Police charged a Warwick man with embezzling $142,114.31 from United States Associates, LLC April 6 following allegations that the suspect was stealing and selling company inventory and keeping the proceeds for himself. An investigation found that the man was receiving checks from one of the company's customers who had been ordering directly from him.
Source: http://warwickpost.com/troopers-arrest-warwick-man-for-embezzling-142k-from-manufacturer/5876/

4. *April 7, U.S. Securities and Exchange Commission* – (California; Ohio) **SEC charges L.A.-based Pacific West Capital Group with fraud in sale of life settlement investments.** The U.S. Securities and Exchange Commission charged Los Angeles-based Pacific West Capital Group Inc., and its owner April 7 with fraud in the sale of life settlement investments for failing to disclose risks associated with the investments and for using the proceeds from the sale of new life settlements to continue funding previously sold investments, raising over $100 million from investors. Ohio-based PWCG Trust and five Pacific West sales agents were also charged in the scheme.
Source: http://www.sec.gov/news/pressrelease/2015-60.html

5. *April 7, WCBS 2 New York City; Associated Press* – (New York) **SEC files fraud charges against former Syracuse star, New York Giant player.** The U.S. Securities and Exchange Commission filed civil fraud charges April 6 against a former National Football League player, his business partner, and Capital Financial Partners investment firms in connection to an alleged Ponzi scheme in which the pair paid approximately $7 million in investors' money instead of using profits from the investments after paying out about $20 million to investors but only receiving around $13 million in loan repayments. The pair also misled investors about the terms and existence of loans and used some funds to cover personal expenses.
Source: http://newyork.cbslocal.com/2015/04/07/former-syracuse-star-new-york-giant-will-allen-charged-with-running-ponzi-scheme/

For another story, see item **22**

[Return to top]

Transportation Systems Sector

6. *April 8, KNBC 4 Los Angeles* – (California) **Tanker crash, fuel spill close freeway for nearly 12 hours.** A stretch of the southbound 605 Freeway in the Lakewood area reopened April 8 after closing for nearly 12 hours following a crash April 7 involving a semi-truck that overturned and spilled 3,500 gallons of gasoline across the roadway after being struck by another vehicle. Two people were transported to an area hospital with injuries.

Source: http://www.nbclosangeles.com/news/local/Tanker-Overturns-on-605-Freeway-in-Long-Beach-299004431.html

7. *April 7, Associated Press* – (Illinois) **Small plane crashes after NCAA title game, killing ISU coach.** The Federal Aviation Administration reported that a twin-engine aircraft traveling from Indianapolis crashed about 2 miles away from the Central Illinois Regional Airport in Bloomington April 7, killing all seven passengers on board. The National Transportation Safety Board is investing the cause of the crash, and stated that the plane was cleared to land in fog and rain but apparently turned away from the approaching runway for an unknown reason before crashing.
Source: http://www.nbc29.com/story/28738328/plane-returning-from-ncaa-game-crashes-in-illinois-7-dead

8. *April 7, Flint Journal* – (Michigan) **Man shot inside MTA bus station in downtown Flint.** The Mass Transit Authority bus station in downtown Flint was closed for several hours April 7 while police investigated a shooting inside the station that left one person injured. The Michigan State Police are searching for the gunman who fled the scene.
Source: http://www.mlive.com/news/flint/index.ssf/2015/04/man_shot_inside_mta_bus_statio.html

9. *April 7, WTOP 103.5 FM Washington, D.C.* – (Virginia) **Water main break closes lanes of Richmond Highway.** A 14-inch water main break at U.S. Route 1/Richmond Highway and Wyngate Court in the Woodlawn area of Fairfax County closed the highway in both directions for 3 hours April 7 before one lane of traffic was reopened in each direction. Crews cut off water service in the area for several hours while repairs were made to the broken pipe.
Source: http://wtop.com/fairfax-county/2015/04/water-main-closes-portion-of-richmond-highway/

For additional stories, see items **1**, **28**, and **30**

[Return to top]

Food and Agriculture Sector

10. *April 8, Associated Press* – (Pennsylvania) **45,000 chickens killed in central Pennsylvania farm fires.** About 32,000 chickens perished in an April 6 fire that caused an estimated $400,000 in damage to a chicken barn and fields at a Heidelberg Township farm. Officials are investigating the April 6 blaze and a second, unrelated fire that destroyed a barn and killed about 13,000 chickens at a Bethel Township farm April 8.
Source: http://abc27.com/ap/45000-chickens-killed-in-central-pennsylvania-farm-fires/

11. *April 8, U.S. Food and Drug Administration* – (National) **Blue Bell Creameries expands recall of products produced in Broken Arrow, Oklahoma due to possible health risk.** Blue Bell Creameries expanded its recall of products that were produced at

its Broken Arrow, Oklahoma plant to include Banana Pudding Ice Cream pints after the U.S. Food and Drug Administration notified the company April 7 that the product tested positive for Listeria monocytogenes. The expansion includes all products that were manufactured on the same production line as the Banana Pudding Ice Cream from February 12 – March 27.
Source: http://www.fda.gov/Safety/Recalls/ucm441620.htm

12. *April 8, U.S. Food and Drug Administration* – (Texas) **Texas Star Nut and Food Co., Inc. expands its voluntary recall to include additional macadamia nut products due to recall notification from their supplier of possible Salmonella contamination.** The U.S. Food and Drug Administration reported April 7 that Texas Star Nut and Food Co. Inc., expanded a March 20 recall to include 3 additional macadamia nut products following a recall notification from a supplier warning of possible Salmonella contamination. The recalled products were distributed to HEB Grocery Stores in Texas.
Source: http://www.fda.gov/Safety/Recalls/ucm441686.htm

13. *April 7, Syracuse Post-Standard* – (New York) **4,000 gallons of liquid manure spill in Broome County after trucker crashes.** About 4,000 gallons of liquid manure spilled onto Caldwell Hill Road and adjacent private property in the town of Lisle April 7 after a semi-truck went off the roadway and overturned into a ditch. The New York State Department of Environmental Conservation Spill Response Team and the New York State Police Commercial Vehicle Enforcement Unit are investigating the incident.
Source:
http://www.syracuse.com/crime/index.ssf/2015/04/4000_gallons_of_liquid_manure_dumps_in_broome_county_after_trucker_crashes.html

14. *April 7, Minneapolis Star Tribune* – (Minnesota) **Eighth Minnesota turkey farm hit with bird flu.** Animal health regulators reported April 7 that the H5N2 bird flu was detected in a flock of 30,000 turkeys in Kandiyohi County, prompting officials to cull the birds and quarantine the farm as a precaution. The Minnesota Animal Health Board and the U.S. Department of Agriculture are working to stop the outbreak that has resulted in the death of 373,000 turkeys in the State, while industry experts are reportedly boosting biosecurity measures.
Source: http://www.startribune.com/lifestyle/health/298939551.html

15. *April 7, U.S. Food and Drug Administration* – (National) **Best Foods Inc. issues allergy alert on undeclared peanuts in Deer Cumin Powder 7 ounce and Deer Cumin Powder 14 ounce.** The U.S. Food and Drug Administration reported April 6 that Best Foods Inc., issued a recall for 7- and 14-ounce packages of Deer brand Cumin Powder due to undeclared peanuts. The recalled products were distributed through retail stores in several States.
Source: http://www.fda.gov/Safety/Recalls/ucm441488.htm

[Return to top]

Water and Wastewater Systems Sector

16. *April 7, Northwest Arkansas Democrat-Gazette* – (Arkansas) **Fort Smith locked in to sewer outlays.** A Federal judge in Fort Smith, Arkansas, signed a consent decree April 6 under which the city of Fort Smith agreed to make nearly $500 million in improvements to its sewer system to eliminate violations of the Clean Water Act and avoid paying thousands of dollars in daily fines. The decree outlines the improvements the city must make, the timeline for when the improvements are to be planned, designed and implemented, and the penalties for failure to meet deadlines.
Source: http://www.nwaonline.com/news/2015/apr/07/fort-smith-locked-in-to-sewer-outlays-2/?news-arkansas-nwa

For another story, see item **9**

[Return to top]

Healthcare and Public Health Sector

17. *April 7, Santa Barbara Independent* – (California) **Clinic may have infected patients with Hepatitis, HIV.** A Santa Barbara County clinic was closed and patients are being identified and contacted by public health officials who are investigating whether clients of the medical office were infected with Hepatitis B, Hepatitis C, or HIV after authorities determined that the clinic was not following standard precautions to protect themselves and patients.
Source: http://www.independent.com/news/2015/apr/07/clinic-may-have-infected-patients-hepatitis-hiv/

[Return to top]

Government Facilities Sector

18. *April 7, Zanesville Times Recorder* – (Ohio) **West Muskingum Middle School evacuated after fire alarm triggered.** Students were evacuated and classes were dismissed at West Muskingum Middle School in Zanesville April 7 after the fire alarm and sprinkler system were triggered by a power surge. Fire crews responded to the school following reports of an oven fire.
Source: http://www.zanesvilletimesrecorder.com/story/news/local/2015/04/07/west-muskingum-middle-school-evacuated-fire-alarm-triggered/25403645/

For additional stories, see items **1**, **22**, and **24**

[Return to top]

Emergency Services Sector

19. *April 7, Tampa Tribune* – (Florida) **Former Tampa police officer pleads guilty in theft of tax refund check.** A former police officer who worked as a corporal at the

Tampa Police Department's Criminal Intelligence Bureau pleaded guilty April 7 to stealing 13 U.S. Department of the Treasury seized tax refund checks worth over $88,000 from the department and cashing them from September 2011 to May 2012.
Source: http://tbo.com/news/crime/former-tampa-police-officer-pleads-guilty-in-theft-of-tax-refund-checks-20150407/

20. *April 7, Rome News-Tribune* – (Georgia) **4 plead guilty to gang activity, riot at Floyd County Jail.** Four inmates at the Floyd County Jail in Rome, Georgia, pleaded guilty to charges in connection to two separate incidents at the jail in November 2013 that allegedly involved gang violence and rioting.
Source: http://www.northwestgeorgianews.com/rome/news/local/plead-guilty-to-gang-activity-riot-at-floyd-county-jail/article_693314cc-dce2-11e4-b38f-c3053328786e.html

[Return to top]

Information Technology Sector

21. *April 8, Softpedia* – (International) **Stored XSS glitch in WP-Super-Cache may affect over 1 million WordPress sites.** Security researchers from Sucuri discovered a cross-site-scripting (XSS) vulnerability in WP-Super-Cache plug-in versions prior to 1.4.4 for WordPress sites that could allow attackers to add new administrator accounts to the Web sites or inject backdoors due to improper sanitization of information originating from users. The plugin currently has over 1 million active installations and developers released a new version repairing the issue.
Source: http://news.softpedia.com/news/Stored-XSS-Glitch-in-WP-Super-Cache-May-Affect-Over-1-Million-WordPress-Sites-477905.shtml

22. *April 8, Threatpost* – (International) **New evasion techniques help AlienSpy RAT spread Citadel malware.** Fidelis researchers reported that hackers have co-opted the AlienSpy remote access tool (RAT) and are spreading it via phishing messages to deliver the Citadel banking trojan and establish backdoors inside a number of critical infrastructure operations, including technology companies, financial institutions, government agencies, and energy companies. The tool has the capability to detect whether it is being executed inside a virtual machine, can disable antivirus and other security tools, and employs transport-layer security (TLS) encryption to protect communication with its command-and-control (C&C) server.
Source: https://threatpost.com/new-evasion-techniques-help-alienspy-rat-spread-citadel-malware/112064

23. *April 8, InfoWorld* – (International) **Widespread outages hit Windows 8/8.1 Metro Mail, Windows Live Mail, Windows Phone 8.1 mail.** Microsoft reported that its Windows 8 and 8.1 Metro Mail, Windows Live Mail, and Windows Phone 8.1 Mail clients were experiencing widespread outages for at least 6 hours April 8 that prevented the syncing and sending of email, and that the issue is expected to be resolved within 24 hours.
Source: http://www.networkworld.com/article/2907300/windows/widespread-outage-for-windows-8-8-1-metro-mail-windows-live-mail-windows-phone-8-1-mail.html

24. *April 7, Securityweek* – (International) **Majority of critical infrastructure firms in Americas have battled hack attempts: Survey.** A report released by Trend Micro and the Organization of the American States revealed that in the last year 40 percent of 575 security leaders throughout critical infrastructure sectors dealt network shut down attempts, while 44 percent faced attempts to delete files, and 60 percent faced hacking attempts aimed at stealing vital information. The survey also found that 54 percent of organizations dealt with attempts of equipment manipulation through control networks or systems.
Source: http://www.securityweek.com/majority-critical-infrastructure-firms-americas-have-battled-hack-attempts-survey

25. *April 7, Softpedia* – (International) **Fake downloads for Android vulnerability scanner lead to persistent ads.** Security researchers at Trend Micro identified three fraudulent Web sites that claim to provide a tool to scan for previously-identified Android Installer hijacking vulnerabilities, which instead redirect users to risky locations that display persistent ads and install Android application package (APK) files on devices automatically.
Source: http://news.softpedia.com/news/Fake-Downloads-for-Android-Vulnerability-Scanner-Lead-to-Persistent-Ads-477843.shtml

26. *April 7, Securityweek* – (International) **Lazy remediation leaves most Global 2000 firms vulnerable after Heartbleed Flaw: Report.** Venafi released new research revealing that as of April 2015, 74 percent of 1,642 Global 2000 organizations with public-facing systems vulnerable to the Open Secure Socket Layer (OpenSSL) Heartbleed flaw failed to fully remediate the risks around the flaw despite warnings and guidance. The study also found that 85 percent of the organizations' external servers were still vulnerable and that 580,000 hosts belonging to them were not completely remediated.
Source: http://www.securityweek.com/lazy-remediation-leaves-most-global-2000-firms-vulnerable-heartbleed-flaw-report

27. *April 7, SC Magazine* – (International) **Drive-by-login attack identified and used in lieu of spear phishing campaigns.** Security researchers at High-Tech Bridge reported that attackers are increasingly utilizing drive-by-logins attacks that target specific visitors to infected Web sites with vulnerabilities that they can leverage to install backdoors that deliver malware directly to users. Researchers believe that these types of attacks are likely to be used in Advanced Persistent Threat (APT) campaigns and could eventually replace phishing attacks.
Source: http://www.scmagazine.com/high-tech-bridge-identifies-new-attack-method-possibly-used-by-apts/article/407805/

28. *April 7, Softpedia* – (International) **Simple FedEx email slips malware on the computer.** Researchers discovered a FedEx phishing campaign that relies on the curiosity of victims to open an attachment in an email purportedly from the company which installs a malware dropper that can steal sensitive data from the system or add it to a network of compromised computers.

Source: http://news.softpedia.com/news/Simple-FedEx-Email-Slips-Malware-on-the-Computer-477837.shtml

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

[Return to top]

Communications Sector

29. *April 7, KREM 2 Spokane* – (Washington) **$200,000 in damage done to Grant Co. cell tower site.** Grant County authorities are investigating after Inland Cellular reported up to $200,000 in damage to a rural cellular phone sire building near Stratford April 2 that was apparently struck by a vehicle on 3 sides of the structure. Electronic equipment housed inside the building was not damaged and cellular service was not interrupted during the incident.
Source: http://www.krem.com/story/news/local/grant-county/2015/04/07/200k-in-damage-done-to-grant-co-cell-tower-site/25434199/

For another story, see item **23**

[Return to top]

Commercial Facilities Sector

30. *April 7, KMOV 4 St. Louis* – (Missouri) **Hail, heavy rain create problems throughout St. Louis area.** Fourteen residents were evacuated from a trailer park in Franklin County after Pin Oak Creek in Villa Ridge overflowed its banks following strong storms that dumped heavy rain and hail across the St. Louis area April 7. Interstate 44 and Interstate 55 were temporarily closed due to weather-related accidents, while a lightning strike caused a Mississippi River traffic signal on the Eads Bridge to malfunction.
Source: http://www.kmov.com/story/28740189/hail-heavy-rain-create-traffic-problems-throughout-st-louis

31. *April 7, Portsmouth Herald* – (New Hampshire) **Seabrook families remain displaced after fire.** About 19 families from Building 1 at the Windjammer Apartment Homes complex in Seabrook are expected to be displaced through April 10 while repairs are made to the fire alarm system, damaged vital electrical wiring, and smoke damaged units following a 2-alarm fire that started in an unoccupied unit April 4. No injuries were reported and the cause of the fire remains under investigation.
Source:
http://www.seacoastonline.com/article/20150407/NEWS/150409363/101115/NEWS

For additional stories, see items **1** and **22**

[Return to top]

Dams Sector

Nothing to report

[Return to top]

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