Homeland Security

Daily Open Source Infrastructure Report
08 December 2015

Top Stories

- Microsoft reported that the company will no longer provide security updates, non-security updates, online content updates, or technical support for older versions of its web browser, Internet Explorer. – *Help Net Security* (See item **28**)

- Researchers reported that Russian-linked hacker group, Pawn Storm, has updated its data theft tools and is utilizing a new version of the AZZY trojan, which is being delivered by another piece of malware instead of a zero-day exploit. – *SecurityWeek* (See item **30**)

- Global law enforcement agencies have partnered with IT companies to disrupt the Dorkbot botnet, dubbed Nrgbot, after the malware spread through multiple channels affecting over a million computers in 190 countries. – *SecurityWeek* (See item **31**)

- South Carolina officials reported December 7 that at least 23 additional broken dams were found in 2 counties and that an additional $7 million was needed to repair roads damaged by the breaks. – *Savannah Morning News* (See item **37**)

Fast Jump Menu

Energy Sector

1. *December 6, WABC 7 New York City* – (New York) **Power restored to approximately 60,000 in Hudson Valley after outage.** Utility crews restored power to nearly 60,000 customers in Hudson Valley December 6 following a substation failure in Middletown that knocked out electricity December 5.
   Source: http://abc7ny.com/news/power-restored-after-outage-affecting-approximately-60000-in-hudson-valley/1111373/

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

2. *December 7, Lower Hudson Valley Journal News* – (New York) **Indian Pt. reactor to remain shut for a couple days.** Entergy Corp. officials reported December 6 that the Unit 2 nuclear reactor at its Indian Point facility will remain offline until December 8 or December 9 following a December 5 power outage that occurred when about 10 control rods dropped into the reactor core, prompting a manual shutdown of the reactor's feedwater pump. Officials reported that no immediate concerns were identified.
   Source: http://www.lohud.com/story/news/local/indian-point/2015/12/05/indian-power-plant-forced-shut-down-reactor-cuomo/76862826/

3. *December 4, Cape Cod Times* – (Massachusetts) **Five more violations found at Pilgrim.** The U.S. Nuclear Regulatory Commission reported December 4 that an October 23 inspection at the Entergy Corp.-owned Pilgrim Nuclear Power Station in Plymouth revealed five violations including failure to recognize and plan for potential mistakes, latent issues, and inherent risks, as well as failure to implement a process of planning, controlling, and executing work activities for nuclear safety.
   Source: http://www.enterprisenews.com/article/20151204/NEWS/151207867

Critical Manufacturing Sector

4. *December 7, WNDU 16 South Bend* – (Indiana) **23 Forest River employees hospitalized after carbon monoxide leak.** The Forest River manufacturing plant in Middlebury was evacuated and 23 employees were taken to area hospitals December 7 due to symptoms of carbon monoxide poisoning following the reported release of carbon monoxide directly into the building after one of the plant's furnaces' exhaust systems rusted.
   Source: http://www.wndu.com/home/headlines/Forest-River-plant-evacuated-after-carbon-monoxide-leak-360789031.html

5. *December 6, WLS 7 Chicago* – (Illinois) **North Side recycling plant fire under investigation.** A December 6 fire at the General Iron Industries metal recycling plant in Chicago is under investigation after fire and HAZMAT crews contained the fire that broke out in a stack of scraps.

Source: http://abc7chicago.com/news/north-side-recycling-plant-fire-under-investigation/1111742/

6. *December 4, Automotive News* – (National) **FCA recalls 121,000 Dodge Darts for brake-related glitch.** Officials from Fiat Chrysler Automobiles issued a recall for 121,000 model year 2013 – 2014 Dodge Dart vehicles due to braking problems stemming from oil migration that could affect the system's power-assist braking feature, leading to longer stopping distances. The company has received two minor injury and seven accident reports that may be related to the issue.
Source: http://www.autonews.com/article/20151204/OEM11/151209914/fca-recalls-121000-dodge-darts-for-brake-related-glitch

7. *December 3, U.S. Department of Labor* – (Pennsylvania) **Portersville, Pennsylvania, manufacturer again cited by OSHA for exposing employees to safety and health hazards.** The Occupational Safety and Health Administration announced December 3 that it issued Portersville Sales & Testing Inc., 15 serious safety and health violations following an investigation December 2 at the company's Portersville, Pennsylvania facility that found improper use of flammable materials and fall hazards, among other violations. Proposed penalties total $43,600.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=29130

For another story, see item **29**

Defense Industrial Base Sector

See item **30**

Financial Services Sector

8. *December 4, SecurityWeek* – (International) **Botnet takes "shotgun" approach to hack PoS systems.** Researchers at Trend Micro reported a new campaign dubbed operation Black Atlas that targets point-of-sale (PoS) systems at small and medium sized businesses and healthcare organizations worldwide utilizing various penetration testing tools including brute force, Simple Mail Transfer Protocol (SMTP) scanners, and remote desktop viewers. Black Atlas received its name from the BlackPOS malware, works in stages, and uses variants of other known malware, allowing hackers to potentially steal sensitive information.
Source: http://www.securityweek.com/botnet-takes-shotgun-approach-hack-pos-systems

9. *December 4, Sacramento Bee* – (California) **Placer County women guilty in multimillion-dollar mortgage fraud scheme.** A Federal jury in Sacramento found 2 Placer County women guilty December 4 for their roles in a mortgage fraud scheme that netted over $16 million and involved more than 30 properties in the Sacramento area that were purchased through straw buyers. The women created fraudulent loan

applications and ran an escrow company used in a majority of the real estate transactions.
Source: http://www.sacbee.com/news/local/crime/article48104005.html

10. *December 4, U.S. Department of Justice* – (Massachusetts) **Two Massachusetts men indicted in massive stolen identity tax refund fraud scheme.** Two Dominican men residing in Massachusetts were charged December 3 for allegedly participating in a scheme to prepare and file fake Federal income tax returns using the stolen identities of more than 800 U.S. citizens including Puerto Rican residents, in order to obtain tax refund checks. The pair also reportedly sold more than 16 tax refund checks valuing over $100,000 to one individual.
Source: http://www.justice.gov/opa/pr/two-massachusetts-men-indicted-massive-stolen-identity-tax-refund-fraud-scheme

Transportation Systems Sector

11. *December 7, WAVY 10 Portsmouth* – (Virginia) **Police ID driver killed in multi-vehicle Chesapeake accident.** Westbound lanes of Route 58 in Chesapeake were closed for several hours December 5 while authorities investigated a multi-vehicle crash that killed 1 person and left another injured.
Source: http://wavy.com/2015/12/05/driver-killed-in-multi-vehicle-accident-in-chesapeake/

12. *December 6, Yankton Daily Press & Dakotan* – (South Dakota) **Saturday accident injures 3, results in power outage.** Old Highway 50 in Yankton reopened after closing for several hours December 5 – 6 while crews cleared the scene after a vehicle crashed into a utility pole, injured 3 people, and knocked out power to various parts of the city.
Source: http://www.yankton.net/community/article_64a20af8-9c9a-11e5-a03f-237e60b05645.html

13. *December 6, Associated Press* – (Oregon) **Hermiston man killed in two-vehicle crash on Highway 207.** Northbound and southbound lanes of Highway 207 in Umatilla County were closed for over 2 hours December 5 while crews cleared the wreckage following a 2-vehicle accident that killed 1 and left another injured.
Source: http://www.lagrandeobserver.com/2015120682930/News/Local-News/Hermiston-man-killed-in-two-vehicle-crash-on-Highway-207

14. *December 6, Fort Worth Star-Telegram* – (Texas) **Crash kills 3 in North Richland Hills.** The westbound lanes of Northeast Loop 820 in North Richland Hills were closed for several hours December 6 after a vehicle crashed into a guardrail and concrete wall and went over onto the highway, killing 3 people.
Source: http://www.star-telegram.com/news/local/community/northeast-tarrant/article48299400.html

15. *December 4, KCRA 3 Sacramento* – (California) **Fairfield police recover stolen mail from 10 NorCal cities.** Two suspects were arrested December 2 at a home in Suisun during a probation search following the discovery of more than 1,000 pieces of stolen

mail from 24 victims across 10 Northern California cities.
Source: http://www.kcra.com/news/fairfield-police-recover-stolen-mail-from-10-norcal-cities/36797422

16. *December 4, Yakima Herald* – (Washington) **Tanker spills 3,000 gallons of gas on I-90, closing highway for nine hours.** Eastbound lanes of Interstate 90 in Kittitas County were closed for approximately 9 hours December 4 after 3,000 gallons of fuel spilled from an overturned semi-truck involved in a multi-vehicle accident that left 2 people injured.
Source: http://www.yakimaherald.com/news/local/tanker-spills-gallons-of-gas-on-i--closing-highway/article_33bb5e02-9a93-11e5-9a70-f71b69881e6e.html

17. *December 4, Los Angeles Times* – (California) **UPS building in San Bernardino deemed safe after suspicious package is checked.** A United Parcel Service, Inc. facility in San Bernardino was evacuated for 3 hours December 4 while authorities investigated and cleared a suspicious package that was addressed to individuals connected to a recent shooting incident.
Source: http://www.latimes.com/local/lanow/la-me-ln-bomb-experts-checking-package-20151204-story.html

18. *December 4, Lompoc Record* – (California) **Fuel truck crash prompts early-morning closure of Hwy. 154; route reopened at 9:30 a.m.** Highway 154 in the Santa Ynez Valley was closed for approximately 9 hours December 4 while crews cleared the scene of an accident involving an overturned semi-truck leaking fuel. HAZMAT crews responded to ensure that the spill was contained.
Source: http://lompocrecord.com/news/local/fuel-truck-crash-prompts-early-morning-closure-of-hwy-route/article_f578a6d4-13cf-5416-a828-bce4eeb965b4.html

Food and Agriculture Sector

19. *December 4, CNN* – (National) **Chipotle E. coli outbreak now linked to illness in 9 states.** The U.S. Centers for Disease Control and Prevention reported December 4 that a widespread outbreak of E. coli linked to food served at Chipotle Mexican Grill, Inc. restaurants spread to 3 more States, including Illinois, Maryland, and Pennsylvania. The outbreak, which began in November and forced the company to revamp its food safety standards, has sickened 52 people and hospitalized 20.
Source: http://www.cnn.com/2015/12/04/health/chipotle-e-coil-update---now-9-states/

Water and Wastewater Systems Sector

20. *December 4, KWTX 10 Waco* – (Texas) **Marlin Water service fully restored; boil order in effect.** Water service was fully restored to most Marlin residents December 4 after large particulates flooded and clogged the filtration system at the city's water treatment plant November 26. A boil advisory remained in effect and residents were advised to conserve water for sanitation use if possible.
Source: http://www.kwtx.com/home/headlines/UPDATE--Marlin-Water-Service-Fully-Restored-360590141.html

Healthcare and Public Health Sector

21. *December 6, Associated Press* – (Indiana) **HIV outbreak in southern Indiana now at 184 cases.** The Indiana State Department of Health reported December 4 that the total number of HIV cases reached 184 in a reported outbreak tied to needle-sharing among individuals injecting a liquefied form of a painkiller in Scott County.
Source: http://ksnt.com/2015/12/06/hiv-outbreak-in-southern-indiana-now-at-184-cases/

22. *December 4, Boston Globe* – (Massachusetts) **Burlington hospital to pay fine after stolen laptop exposed patient data.** Lahey Hospital & Medical Center in Burlington will pay $850,000 in a settlement reached with the U.S. Department of Health and Human Services December 4 after a laptop containing personal and medical information on approximately 599 patients was stolen from an unlocked treatment room in August 2011. The hospital will also implement a corrective action plan to improve security measures.
Source: https://www.bostonglobe.com/business/2015/12/04/lahey-hospital-pay-fine-after-stolen-laptop-exposed-patient-information/HWxW2xS1diOhu8jSPXAoCL/story.html

For another story, see item **8**

Government Facilities Sector

See item **30**

Emergency Services Sector

23. *December 7, WLS 7 Chicago* – (Illinois) **U.S. Dept. of Justice to investigate Chicago Police Department.** The U.S. Department of Justice announced December 7 that it launched an investigation into the Chicago Police Department to determine if the department uses patterns of violence that violates Federal law following an October 2014 officer-involved shooting death of a teenager.
Source: http://abc7chicago.com/news/us-dept-of-justice-to-investigate-cpd-/1112453/

24. *December 7, Chicago Tribune* – (Illinois) **2 inmates, one from Chicago, escape from southern Illinois prison.** Authorities are searching for two inmates who escaped from the Dixon Springs Impact Incarceration Program, an Illinois State prison facility, December 6.
Source: http://www.chicagotribune.com/news/local/breaking/ct-idoc-2-escape-including-man-from-chicago-from-southern-illinois-prison-20151206-story.html

25. *December 6, WRC 4 Washington, D.C.* – (Washington, D.C.) **Person takes grenade to D.C. police station.** The Metropolitan Police Department's Fourth District police station in Washington, D.C., along with two surrounding businesses, were evacuated for more than 4 hours December 6 after a citizen arrived at the station with a hand grenade. Police rendered the device safe after removing it from the individual's vehicle

for disposal.
Source: http://www.nbcwashington.com/news/local/Person-Takes-Grenade-to-DC-Police-Station-360719441.html

26. *December 5, KCBS 2 Los Angeles* – (California) **At least 10 inmates injured in fight at Men's Central Jail, no deputies hurt.** The Men's Central Jail in Los Angeles was locked down following a fight involving about 120 inmates that left at least 10 inmates injured December 4. Authorities used pepper-spray to quell the disturbance and restore order.
Source: http://losangeles.cbslocal.com/2015/12/05/10-inmates-injured-in-fight-at-mens-central-jail-no-deputies-hurt/

Information Technology Sector

27. *December 7, Softpedia* – (International) **Trifecta of security bugs affecting Dell, Lenovo, and Toshiba products.** Security researchers from LizardHQ reported that three major security vulnerabilities were affecting current and older versions of computer products including Dell System Detect, Lenovo's Solution Center, and Toshiba Service Station that allows attackers to abuse an application program interface (API) to bypass the Windows User Account Control limitations on Dell products, run malicious code and escalate privileges to administrative rights on Lenovo products, and allows attackers to read parts of the Windows registry as a SYSTEM-level users in Toshiba products. The companies released recommendations on how to fix the vulnerabilities.
Source: http://news.softpedia.com/news/trifecta-of-security-bugs-affecting-dell-lenovo-and-toshiba-products-497226.shtml

28. *December 7, Help Net Security* – (International) **Microsoft warns of imminent end of support for all but the latest Internet Explorer versions.** Microsoft reported that the company will no longer provide security updates, non-security updates, online content updates, or technical support for older versions of its web browser, Internet Explorer in an attempt to encourage users to upgrade from Internet Explorer 11 to Microsoft Edge and Windows 10.
Source: http://www.net-security.org/secworld.php?id=19197

29. *December 7, SecurityWeek* – (International) **Serious flaws found in Honeywell gas detectors.** Honeywell released firmware updates to it Midas gas detectors after a security researcher discovered that Midas gas detectors running firmware versions 1.13b1 and older, and Midas Black products running firmware versions 2.13b1 and older, were susceptible to a path traversal flaw and a clear text flaw that can be exploited remotely by an attacker with low skill by typing a targeted Uniform Resource Locator (URL) into the device to bypass authentication procedures.
Source: http://www.securityweek.com/serious-flaws-found-honeywell-gas-detectors

30. *December 7, SecurityWeek* – (International) **Russian cyberspies use updated arsenal to attack defense contractors.** Researchers from Kaspersky Lab reported that Russian-linked cyber espionage group, Pawn Storm, which targets international military, media,

defense, and government organizations has updated its data theft tools and is utilizing a new version of the AZZY trojan which is being delivered by another piece of malware instead of a zero-day exploit. The new AZZY backdoor also uses an external library for command and control (C&C) communications.
Source: http://www.securityweek.com/russian-cyberspies-use-updated-arsenal-attack-defense-contractors

31. *December 4, SecurityWeek* – (International) **International operation disrupts dorkbot botnet.** Global law enforcement agencies have partnered with Microsoft, ESET, and CERT Polska to disrupt the Dorkbot botnet, dubbed Nrgbot, after the malware spread through multiple channels, including Universal Serial Bus (USB) flash drives, instant messaging programs, social network sites, exploit kits (EK), and spam emails, affecting over a million computers in 190 countries. Researchers advised users to keep their antivirus programs updated at all times to ensure proper protection from the malware that steals personal information and credentials and distributes other forms of malware.
Source: http://www.securityweek.com/international-operation-disrupts-dorkbot-botnet

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

32. *December 5, Fort Worth Star-Telegram* – (Texas) **30 displaced, 9 injured in Euless apartment fire.** A 2-alarm fire at The Palisades at Break Creek apartments in Euless, Texas, displaced 30 people, damaged 8 apartment units, and injured 9 people December 5. Fire crews contained the incident and the cause of the fire was undetermined.
Source: http://www.star-telegram.com/news/local/community/northeast-tarrant/article48175325.html

33. *December 5, Forum of Fargo-Moorhead* – (North Dakota) **Fire forces evacuation of retirement center in Casselton.** A December 5 fire at Casselwood Retirement Center in North Dakota prompted an evacuation of the building and displaced 21 residents. Officials are investigating the cause of the fire and reported that the facility will be closed until further notice.
Source: http://www.inforum.com/news/3897363-fire-forces-evacuation-retirement-center-casselton

34. *December 4, WRC 4 Washington* – (Virginia) **Manassas Mall reopening after**

evacuation as precaution for police search. Prince William County Police reported that the Manassas Mall in Virginia reopened December 4 after the mall was evacuated for over 3 hours as a precaution while police searched the mall following a bomb threat. No explosive devices were found.
Source: http://www.nbcwashington.com/news/local/Manassas-Mall-Evacuated-as-a-Precaution-for-Police-Search-360572661.html

35. *December 4, WTTG 5 Washington, D.C.* – (California) **Fire in parking garage prompts evacuation of Hillcrest apartments.** The San Diego Fire-Rescue Department reported December 4 that a vehicle fire in an underground parking garage of a Hillcrest apartment complex prompted residents to evacuate. The cause of the fire is under investigation and the total amount of damages was estimated at $600,000.
Source: http://fox5sandiego.com/2015/12/04/fire-in-parking-garage-prompts-evacuation-of-hillcrest-apartments/

For another story, see item **25**

Dams Sector

36. *December 7, Savannah Morning News* – (South Carolina) **2 months after storm, breached dams still found in S.C.** South Carolina officials reported December 7 that at least 23 additional broken dams were found in Richland and Lexington counties and that an additional $7 million was needed to repair roads damaged by the breaks, which could take a year to complete.
Source: http://savannahnow.com/news/2015-12-07/2-months-after-storm-breached-dams-still-found-sc#

37. *December 5, Marysville Appeal-Democrat* – (California) **8.5 million funds more levee work in Sutter County.** A mile of levee upgrades was added to the Feather River West Levee project in Sutter County, pending $8.5 million in funding received from California. The project will help raise flood protection in urban and rural areas.
Source: http://www.appeal-democrat.com/news/million-funds-more-levee-work-in-sutter-county/article_9d73c2b0-9ba8-11e5-9ee0-0f56ff698cd9.html

38. *December 4, Baltimore Sun* – (Maryland) **Centennial Lake water level to be lowered for dam cleaning, repairs.** The Howard County Department of Recreation & Parks stated December 4 that it will be lowering the water level of Ellicott City's Centennial Lake by 6 inches each day until water levels reach 5 feet in depth, prior to the December 17 estimated start date of repairs to the dam's structure.
Source: http://www.baltimoresun.com/news/maryland/howard/ellicott-city/ph-ho-cf-centennial-lake-lowered-repairs-1210-20151204-story.html

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.