Daily Open Source Infrastructure Report
15 December 2016

Top Stories

- Thirty-five individuals connected to the Brooklyn, New York-based Hoodstarz street gang and associated crews were charged December 13 for allegedly buying more than 750 credit card numbers from the Dark Web and using the numbers to create fraudulent credit cards. – *WNBC 4 New York* (See item **5**)
- A Nigerian national pleaded guilty December 12 for his role in a roughly $4.7 million scheme to file thousands of fraudulent Federal and Oregon State tax returns from 2012 – 2015. – *Medford Mail Tribune* (See item **6**)
- The Stamford Water Pollution Control Authority in Connecticut reported that 84,000 gallons of raw sewage leaked into the East Branch of Stamford Harbor December 13. – *Stamford Advocate* (See item **15**)
- Frederick County Public Schools officials in Maryland announced December 13 that the personal information of about 1,000 former students was stolen and offered for sale online following a data breach that occurred before 2010. – *Frederick News-Post* (See item **17**)

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. *December 13, KWCH 12 Hutchinson* – (Kansas) **OSHA investigating explosion at Wallace County oil-drilling site.** The Occupational Safety and Health Administration is investigating after a December 12 explosion at a Murfin Drilling Company, Inc. oil-drilling site near Sharon Springs, Kansas, that injured five workers.
   Source: http://www.kwch.com/content/news/Five-hurt-two-critically-in-Wallace-County-gas-explosion-406086335.html

For another story, see item **9**

Chemical Industry Sector

See item **27**

Nuclear Reactors, Materials, and Waste Sector

2. *December 13, Asbury Park Press* – (New Jersey) **Oyster Creek nuclear plant taken offline.** Exelon Corp. officials announced that the Oyster Creek Nuclear Generating Station in Lacey Township, New Jersey, was taken offline December 13 in order to complete repairs to the plant's turbine control system, which monitors turbine conditions, speed, temperature, and pressure. Officials reported the shutdown would not impact electrical service to Exelon customers.
   Source: http://www.app.com/story/news/local/land-environment/2016/12/13/oyster-creek-nuclear-plant-taken-offline/95389556/

Critical Manufacturing Sector

3. *December 13, Bucyrus Telegraph-Forum* – (Ohio) **Blaze damages New Washington business.** Mansfield Aluminum Castings in New Washington, Ohio, was closed until further notice December 13 following a fire that caused significant damage to the facility. No injuries were reported.
   Source: http://www.bucyrustelegraphforum.com/story/news/local/2016/12/13/fire-reported-new-washington-company/95367142/

4. *December 12, Washington Post* – (California) **A Calif. man steals $5 million, spends $1 million on a cellphone game.** A California man pleaded guilty December 8 after he defrauded his employer, Holt Manufacturing Company, out of nearly $5 million from May 2008 – March 2015 by conducting hundreds of unauthorized credit card transactions on the firm's commercial account, falsifying records regarding the account, and misleading the bank that held the credit account when it made inquiries about suspicious transactions. The former employee used the stolen funds for personal expenses.
   Source: https://www.washingtonpost.com/news/morning-mix/wp/2016/12/12/a-calif-man-stole-nearly-5-million-from-his-company-then-spent-1-million-on-a-cellphone-game/?utm_term=.1eab2b6b5a60

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *December 14, WNBC 4 New York* – (New York) **Brooklyn gang members used fake credit cards to buy American Girl dolls, guns: Officials.** Thirty-five individuals connected to the Brooklyn, New York-based Hoodstarz street gang and associated crews were charged December 13 for allegedly buying more than 750 credit card numbers from the Dark Web and using the numbers to create fraudulent credit cards, which the group used to buy dolls, concert tickets, and weapons, as well as to fund violent crimes. The charges allege that the group tested the fraudulent credit cards by charging $1 at parking meters.
   Source: http://www.nbcnewyork.com/news/local/Fake-Credit-Card-Brooklyn-Gang-Indictment-Violence-American-Girl-Dolls-Hoodstarz-406312075.html

6. *December 14, Medford Mail Tribune* – (International) **Stolen PINs net nearly $5 million in tax fraud.** A Nigerian national pleaded guilty December 12 for his role in a roughly $4.7 million scheme to file thousands of fraudulent Federal and Oregon State tax returns from 2012 – May 2015 where he and 5 co-conspirators obtained the personal information of more than 250,000 people from an overseas hacker, and used the information to get PIN numbers used by the victims to electronically file U.S. Internal Revenue Service (IRS) returns. The IRS paid refunds directly to prepaid debit cards or third-party bank accounts the group opened, and the co-conspirators subsequently wired some of the refunds to Nigeria via the Western Union Company.
   Source: http://www.mailtribune.com/news/20161213/stolen-pins-net-nearly-5-million-in-tax-fraud

For another story, see item **4**

Transportation Systems Sector

7. *December 14, Allentown Morning Call* – (Pennsylvania) **I-80 closed in Monroe County as troopers recreate triple-fatal crash.** Westbound lanes of Interstate 80 in Monroe County, Pennsylvania, were closed for 4 hours December 14 while State officials worked to reconstruct a fatal crash that killed 3 people.
   Source: http://www.mcall.com/news/local/police/mc-monroe-highway-closure-20161214-story.html

8. *December 14, WTTG 5 Washington, D.C.* – (Maryland) **13-year-old boy killed in accident that closed Interstate 95.** Both directions of Interstate 95 in Beltsville, Maryland, were closed for 5 hours December 13 – December 14 while officials investigated a collision involving at least 4 vehicles that killed 1 person and injured several others.
   Source: http://www.fox5dc.com/news/local-news/223528126-story

9. *December 14, WCBS 2 New York; Associated Press* – (New Jersey) **Overturned tanker spills fuel onto roadway, snarls traffic in Linden.** Northbound lanes of U.S. Routes 1 and 9 in Linden, New Jersey, were closed for almost 8 hours December 14 while HAZMAT crews worked to clean a 1,900-gallon diesel spill after a semi-truck struck the center median and overturned.
Source: http://newyork.cbslocal.com/2016/12/14/linden-overturned-tanker/

10. *December 14, Bloomington Pantagraph* – (Illinois) **Sneeze causes 2-vehicle crash near Atlanta.** Interstate 55 near Atlanta, Illinois, was closed for about 5 hours December 13 while officials worked to clear the wreckage after a collision involving 2 semi-trucks that caused 1 of the trucks to strike the guardrail and overturn. One driver was injured.
Source: http://www.pantagraph.com/news/local/sneeze-causes--vehicle-crash-near-atlanta/article_6600c296-cc1a-5f41-9391-f85d2ad0f3d4.html

11. *December 14, Santa Rosa Press Democrat* – (California) **Chlorine spill forces hours-long closure of Highway 12 near Sebastopol.** Westbound lanes of California State Route 12 near Sebastopol were closed for over 3 hours December 13 while HAZMAT crews worked to clean up liquid chlorine that spilled on the roadway after 36 one-gallon containers of chlorine rolled off a truck.
Source: http://www.pressdemocrat.com/news/local/6430187-181/chlorine-spill-closes-westbound-highway?artslide=0

12. *December 13, Associated Press* – (Connecticut) **Connecticut bulk mail executive pleads guilty to fraud.** The operator of Connecticut-based Creative Marketing Group LLC pleaded guilty to stealing $750,000 worth of postage for his company by using false documentation that indicated he had already paid for the mailings through an advanced deposit account in order to send out more than 3.2 million pieces of mail without paying for the postage.
Source: http://www.theday.com/statenortheast/20161213/connecticut-bulk-mail-executive-pleads-guilty-to-fraud

13. *December 13, West Kentucky Star* – (Kentucky) **Nine hurt in PATS bus accident.** Nine people were transported to area hospitals after a Paducah Area Transit System bus was rear-ended on Park Avenue between 32nd Street and Levin Avenue in Paducah, Kentucky, December 13.
Source: http://www.westkentuckystar.com/News/Local-Regional/McCracken-County/Nine-Hurt-in-PATS-Bus-Accident.aspx

Food and Agriculture Sector

14. *December 13, U.S. Food and Drug Administration* – (National) **Linden Cookies issues allergy alert on undeclared milk in mini chocolate chip cookies and 3 pack chocolate chip cookies.** Linden Cookies, Inc. issued a recall December 13 for its fully baked Linden's Chocolate Chip Cookies products sold in 3 variations due to mislabeling and undeclared milk after being notified by the chocolate chip manufacturer that the raw ingredient contains undeclared milk. No illnesses or adverse

reactions have been reported and the products were shipped to wholesalers in 8 States.
Source: http://www.fda.gov/Safety/Recalls/ucm533159.htm

Water and Wastewater Systems Sector

15. *December 14, Stamford Advocate* – (Connecticut) **Broken pipe leaks 84,000 gallons of sewage into Stamford Harbor.** The Stamford Water Pollution Control Authority in Connecticut reported that 84,000 gallons of raw sewage leaked into the East Branch of Stamford Harbor December 13 after a force main pipe broke at the city's water pollution control plant. Officials stated that the spill has been contained and the pipe is being repaired.
Source: http://www.stamfordadvocate.com/local/article/Broken-pipe-leaks-84-000-gallons-of-sewage-into-10795509.php

Healthcare and Public Health Sector

16. *December 13, Gainesville Sun* – (Florida) **Vet, 60, charged after Villages VA shooting thwarted.** Up to 400 people were evacuated from The Villages Veterans Affairs (VA) Clinic in Florida December 13 after a veteran opened fire inside the facility, forcing the closure of the facility until December 14. The shooter was arrested after being disarmed by staff members and patients and no injuries were reported.
Source: http://www.gainesville.com/news/20161213/vet-60-charged-after-villages-va-shooting-thwarted

Government Facilities Sector

17. *December 13, Frederick News-Post* – (Maryland) **Personal details of about 1,000 former Frederick County students stolen, was for sale.** A spokesperson for Frederick County Public Schools in Maryland announced December 13 that the personal information of about 1,000 former students who attended the district's schools between November 2005 and November 2006 was stolen and offered for sale online following a data breach that occurred before 2010. The breach was discovered in September when a former student found the information online.
Source: http://www.fredericknewspost.com/news/education/schools/personal-details-of-about-former-frederick-county-students-stolen-was/article_147339b1-de16-513b-8288-0e0ba62bf506.html

Emergency Services Sector

Nothing to report

Information Technology Sector

18. *December 14, SecurityWeek* – (International) **Apple patches 72 vulnerabilities in macOS Sierra.** Apple released version 10.12.2 of its Sierra operating system (OS) patching a total of 72 vulnerabilities in Apache, Audio, Bluetooth, security, the kernel, and Disk Images, among other components, after security researchers discovered that

the flaws could be exploited to cause an application to enter a denial-of-service (DoS) condition, execute arbitrary code with elevated privileges, leak memory data, and overwrite existing files, among other nefarious actions. Apple also released security updates for iCloud for Microsoft Windows, iTunes for Windows, and Safari 10.0.2, which resolved two dozen flaws.
Source: http://www.securityweek.com/apple-patches-72-vulnerabilities-macos-sierra

19. *December 14, SecurityWeek* – (International) **Microsoft patches several publicly disclosed flaws.** Microsoft released its December 2016 security updates which include a total of 12 critical and important security bulletins that resolve flaws in Windows, Office, Edge, and Internet Explorer, including 11 flaws in Edge, an information disclosure and 2 remote code execution bugs in Windows graphics component, and 16 privilege escalation, information disclosure, and arbitrary code execution flaws, among other flaws, in Office and Office for Apple Mac. One of the critical bulletins also includes patches for Adobe Flash Player, in which Adobe resolved a total of 17 vulnerabilities, including a zero-day flaw that was being exploited in targeted attacks.
Source: http://www.securityweek.com/microsoft-patches-several-publicly-disclosed-flaws

20. *December 14, Help Net Security* – (International) **Corporate Office 365 users hit with clever phishing attack.** Security researchers reported that phishers are targeting users of Microsoft's Corporate Office 365 service to bypass its email filters and default security protections using a trick that makes the user see one Uniform Resource Locator (URL) in the link and anti-phishing filters another link, while the actual link leads the victim to a third, phishing URL. The malicious actors exploit the way that Office 365 anti-phishing and URL-reputation security layers translate Punycode, the method for encoding domain names with Unicode characters.
Source: https://www.helpnetsecurity.com/2016/12/14/corporate-office-365-phishing/

21. *December 13, Help Net Security* – (International) **More Android-powered devices found with trojans in their firmware.** Doctor Web security researchers discovered two types of downloader trojans incorporated in the firmware of several Android-powered devices that are used to deliver ad-showing apps that push users to download additional apps, and are capable of updating themselves, contacting their command and control (C&C) servers, receiving instructions on which apps to covertly download and run, and start running each time the device is turned on. One of the trojans, dubbed Android.Sprovider.7 was found inserted into the firmware of Lenovo smartphones and can open specified links in a browser, as well as show ads on top of apps and in the status bar, among other malicious actions.
Source: https://www.helpnetsecurity.com/2016/12/13/android-devices-trojans-firmware/

22. *December 13, Help Net Security* – (International) **93% of SOC managers unable to triage all potential threats.** Intel Security released a report after interviewing 400 Security Operations Center (SOC) managers across several countries, industries, and company sizes, which revealed that on average, organizations are unable to adequately

investigate 25 percent of security alerts, as many as 93 percent of SOCs are unable to triage all potential threats, and that the most common threat detection signals for 64 percent of companies come from traditional security control points, including firewall and intrusion prevention systems, among other findings.
Source: https://www.helpnetsecurity.com/2016/12/13/soc-managers-triage-threats/

23. *December 13, SecurityWeek* – (International) **Apple patches 12 vulnerabilities in iOS, tvOS, and watchOS.** Apple released version 10.2 of its mobile operating system (iOS) resolving 12 vulnerabilities affecting several components in iPhone 5 and later, iPad 4th generation and later, and iPod touch 6th generation and later, including a memory corruption issue in the Profiles component, which was also found to impact 4th generation Apple TV and all Apple Watch models, that could allow an attacker to achieve arbitrary code execution if the victim opened a specially crafted certificate on a vulnerable device.
Source: http://www.securityweek.com/apple-patches-12-vulnerabilities-ios-tvos-and-watchos

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. *December 14, Help Net Security* – (International) **Netgear pushes out beta firmware for vulnerable router models.** Netgear released a beta firmware to temporarily resolve a vulnerability affecting at least 12 of its router models after confirming the flaw could allow remote, unauthenticated attackers to execute Linux commands with root privileges on the routers if the commands are appended to the Uniform Resource Locator (URL) of a page that the user is tricked into visiting. Netgear is reviewing its router portfolio to determine if the flaw affects other router models.
Source: https://www.helpnetsecurity.com/2016/12/13/netgear-firmware-vulnerable-routers/

Commercial Facilities Sector

25. *December 14, KCBS 740 AM San Francisco; San Francisco Bay City News* – (California) **Four-alarm fire destroys Santa Rosa warehouse.** A 4-alarm fire in Santa Rosa, California, caused significant damage to a warehouse serving Copperfield's Books Inc. and other businesses December 14. No injuries were reported and the cause of the fire remains under investigation.
Source: http://sanfrancisco.cbslocal.com/2016/12/14/four-alarm-fire-destroys-santa-rosa-warehouse/

26. *December 13, Biloxi Sun Herald* – (Mississippi) **Edgewater Mall evacuated after**

smoke fills entrance. The Edgewater Mall in Biloxi, Mississippi, was evacuated December 13 after smoke from an air conditioning unit filled the building. Mall officials planned to reopen the facility December 14.
Source: http://www.sunherald.com/news/local/counties/harrison-county/article120737778.html

27. *December 12, Gephardt Daily* – (Utah) **Discovery Gateway evacuated as crews investigate suspected chemical spill.** The Discovery Gateway children's museum in Salt Lake City was evacuated December 12 while HAZMAT crews investigated a chemical spill involving glycol. No injuries were reported and authorities believe the spill came from the HVAC system.
Source: http://gephardtdaily.com/local/discovery-gateway-evacuated-as-crews-investigate-suspected-chemical-spill/

Dams Sector

28. *December 13, Pittsburgh Post-Gazette* – (Ohio) **Malfunction in hydraulic system shuts down lock on Ohio River.** The U.S. Army Corps of Engineers reported that a hydraulic system at the New Cumberland Locks and Dam near Wellsville, Ohio, failed December 13, halting Ohio River traffic and forcing a section of the river to be closed. Officials stated the lock will be out of service for several days while crews develop a temporary fix that will allow river traffic to resume.
Source: http://www.post-gazette.com/business/pittsburgh-company-news/2016/12/13/Busted-lock-halts-Ohio-River-traffic-near-Wellsville-Ohio/stories/201612130162

29. *December 13, WTVD 11 Durham* – (North Carolina) **Fayetteville dam breach has neighborhood on alert.** The North Carolina Department of Environmental Quality Division of Dam Safety notified Cumberland County's Emergency Management Services December 9 that the Gables Drive Dam in Fayetteville breached, causing water to overtop the dam and prompting the county to issue a Code Red to 40 Country Club Hills homeowners advising them of a potential risk of flooding. Officials reported that a clogged drain pipe filled with storm debris caused the breach and 2,200 gallons of water are being removed per minute in order to lower the lake by a foot each day.
Source: http://abc11.com/news/fayetteville-dam-breach-has-neighborhood-on-alert/1655111/

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