Daily Open Source Infrastructure Report
24 January 2014

Top Stories

- The U.S. Department of Justice accused Virginia-based US Investigations Services LLC of defrauding the federal government of millions of dollars by filing more than 660,000 flawed background investigations. – *United Press International* (See item **13**)

- An analysis of 139 U.S. retailers found 1,035 instances of unique malware infections actively communicating with attackers, averaging 7.5 infections per company. – *The Register* (See item **21**)

- Two people were hospitalized and one firefighter was injured after a drug lab exploded at a California apartment complex, leaving at least 146 residents displaced. – *KTXL 40 Sacramento* (See item **30**)

- A man was charged with setting at least 10 fires that damaged 3 apartment complexes and a car at an auto dealership in Santa Monica. – *Los Angeles Times* (See item **34**)

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. *January 23, Norfolk Virginian-Pilot* – (Virginia; North Carolina) **Scattered power outages continue in Va., N.C.** Utility crews restored power January 22 to more than 23,000 customers in southeastern Virginia and northeastern North Carolina that lost service during a severe snowstorm January 21.
Source: http://hamptonroads.com/2014/01/scattered-power-outages-continue-va-nc

For another story, see item **4**

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

2. *January 23, Rutland Herald* – (Vermont) **Yankee blows fuse, reduces power.** The operators of the Vermont Yankee nuclear power plant in Vernon reduced power January 22 after a fuse located in an electrical control circuit for the condenser steam jet air ejectors blew out. The fuse was replaced and the plant returned to full power after about 6 hours.
Source: http://rutlandherald.com/article/20140123/THISJUSTIN/701239926/0/NEWS01

3. *January 22, Baltimore Sun* – (Maryland) **Electric malfunction shuts down Calvert Co. power plant.** The Calvert Cliffs nuclear power plant near Lusby was shut down January 21due to an electrical malfunction in the non-nuclear side of the plant. The plant's operators believe the incident was caused by snow and ice that impacted a ventilation system and caused a tripped breaker.
Source: http://www.baltimoresun.com/business/bs-md-power-plant-closure-20140122,0,4226643.story

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

4. *January 23, Softpedia* – (International) **Mining pool "Give Me Coins" hacked, 10,000 Litecoins stolen.** The administrators of the Give Me Coins virtual currency mining pool stated that the service was compromised by attackers who stole around $230,000 worth of the Litecoin virtual currency. The attackers were believed to have used a SQL injection vulnerability to breach the service.
Source: http://news.softpedia.com/news/Mining-Pool-Give-Me-Coins-Hacked-10-000-Litecoins-Stolen-419921.shtml

5. *January 21, Denver Post* – (Colorado) **FDIC sues former execs of United Western Bank to recover on questionable loans.** The Federal Deposit Insurance Corporation filed a lawsuit against six former officers and three former directors of the failed United Western Bank, seeking damages related to questionable loans that defaulted and caused $35 million in losses to the bank.
Source: http://www.denverpost.com/portal/business/ci_24961568/fdic-sues-ex-uwb-execs-recover-questionable-loans?_loopback=1

For another story, see item **21**

Transportation Systems Sector

6. *January 23, Martins Ferry Times Leader* – (Ohio) **Tanker accident closes Ohio 78.** A propane tanker rolled over January 22 on Ohio 78 in Monroe County and closed down the road for several hours. No spills or injuries were reported.
Source: http://www.timesleaderonline.com/page/content.detail/id/552140/Tanker-accident-closes-Ohio-78.html?nav=5010

7. *January 22, Newark Star-Ledger* – (New Jersey) **NJ Transit, Amtrak trains bypassing Newark Airport rail station after burst water pipe.** New Jersey Transit and Amtrak trains bypassed the Newark Liberty International Airport stop due to a burst water pipe at the station that required emergency maintenance January 22. Additional bus services were added to help customers reach their destinations.
Source: http://www.nj.com/news/index.ssf/2014/01/nj_transit_amtrak_trains_bypassing_newark_airport_rail_station_after_burst_water_pipe.html

Food and Agriculture Sector

8. *January 22, Food Safety News* – (South Dakota) **Listeria contamination found in raw milk from South Dakota dairy farm.** The South Dakota Department of Agriculture announced that bottled raw milk from Jerseydale Farms near Brookings, South Dakota, tested positive for Listeria and should be discarded or returned. The unpasteurized milk was sold in the Brookings area, which includes the South Dakota State University campus.
Source: http://www.foodsafetynews.com/2014/01/state-tests-find-listeria-contamination-in-raw-milk-from-south-dakota-dairy-farm/

9. *January 22, U.S. Food and Drug Administration* – (National) **Lochiel Enterprises Limited recalls St Mary's River Smokehouses Oven Smoked Salmon Stix, Chili Mango Flavor because of possible health risk.** The U.S. Food and Drug administration announced January 22 that Lochiel Enterprises Limited of Sherbrooke, Nova Scotia recalled 56 pounds of St. Mary's River Smokehouses Oven Smoked Salmon Stix, Chili Mango Flavor due to possible Listeria contamination. The salmon product was distributed to retail stores in Maine, New Hampshire, Massachusetts, Vermont, and New York.
Source: http://www.fda.gov/Safety/Recalls/ucm382537.htm

[Return to top]

Water and Wastewater Systems Sector

10. *January 22, Canton Daily Ledger* – (Illinois) **Boil order issued in Canton following water main break**. A water main break January 21 led to a boil order advisory for residents in Canton, including two local medical facilities, until further notice.
Source:http://www.cantondailyledger.com/article/20140122/NEWS/140129656/-1/sports

11. *January 22, KGTV 10 San Diego* – (California) **Water main breaks on Murphy Canyon Rd.** A private contractor accidentally ruptured a 12-inch pipeline in San Diego January 22 and flooded a street, forcing detours and leaving nearby office buildings without water service for several hours.
Source: http://www.10news.com/news/water-main-break-in-murphy-canyon-area-012214

[Return to top]

Healthcare and Public Health Sector

12. *January 22, Gaston Gazette* – (North Carolina) **CaroMont employee loses patient information in theft.** CaroMont Health announced January 22 that paper records containing personal information of 191 patients of CaroMont Regional Medical Center in Gastonia were stolen in December 2013 from an employee's vehicle in Dallas, North Carolina. Authorities continue to investigate the incident and the hospital has since

retrained their employees on patient privacy practices.
Source: http://www.gastongazette.com/spotlight/caromont-employee-loses-patient-information-in-theft-1.266048?page=0

[Return to top]

Government Facilities Sector

13. *January 23, United Press International* – (National) **U.S. accuses firm that vetted NSA contractor of fraud.** The U.S. Department of Justice accused Virginia-based US Investigations Services LLC of defrauding the federal government of millions of dollars by filing more than 660,000 flawed background investigations. The company is accused of rushing improperly reviewed background checks through the system and hiding a dumping practice from authorities.
Source: http://www.upi.com/Top_News/US/2014/01/23/US-accuses-firm-that-vetted-Snowden-of-fraud/UPI-84301390458900/

14. *January 22, Miami Herald; South Florida Sun-Sentinel* – (Florida) **Shooting scare at Miramar Town Center leaves one dead; three suspects questioned by police.** The city hall, a library, community college, and arts center in Miramar Town Center in Florida were shut down for more than 3 hours January 22 while police questioned 3 suspects in a shooting death near the complex.
Source: http://www.miamiherald.com/2014/01/22/3885751/shooting-near-miramar-city-hall.html

15. *January 23, Baltimore Sun* – (Maryland) **Howard schools recover from possible cyber attack.** Officials from the Howard County Public School System in Maryland are investigating a possible cyberattack that may have caused intermittent Internet outages at various schools that persisted over the course of a week in January.
Source: http://www.baltimoresun.com/news/maryland/howard/ellicott-city/ph-ho-cf-hcpss-internet-0123-20140121,0,3898276.story

16. *January 22, Associated Press* – (New Mexico) **Northern NM charter school classes canceled amid 'general threat.'** McCurdy Charter School in Espanola cancelled classes as a precaution January 22 after the school received a threat allegedly warning students not to attend classes. Authorities are investigating the validity of the threat.
Source: http://www.tribtown.com/view/story/3cfed1f3cf514308932db85db3ebb538/NM--School-Closure-Threat

17. *January 22, WSMV 4 Nashville* – (Tennessee) **Propane shortage closes schools, keeps homes frigid.** Schools in Stewart County, Tennessee, were closed January 23-24 due to a propane shortage that limited the supply available to heat the schools.
Source: http://www.wsmv.com/story/24523058/propane-shortage-closes-schools-keeps-homes-frigid

18. *January 21, WBUP 10 Ishpeming* – (Michigan) **NMU Learning Resource Center**

reopens after water main break. A water main break January 21 led to the temporary closure of Northern Michigan University's Learning Resource Center and caused a campus-wide Internet, phone, and email service outage for more than 7 hours.
Source: http://abc10up.com/nmu-learning-resource-center-temporarily-closed/

Emergency Services Sector

19. *January 22, Corpus Christi Caller-Times* – (Texas) **911 calls system back to normal, police say.** The 9-1-1 emergency system for Corpus Christi and surround cities was down for about 2 hours January 22 after a commercial power transformer disrupted power at AT&T's central office.
Source: http://www.caller.com/news/2014/jan/22/911-service-out-area-police-say/

Information Technology Sector

20. *January 23, Softpedia* – (International) **Snapchat's account registration CAPTCHA system hacked.** Two researchers separately reported that they developed scripts to automate the solving of Snapchat's CAPTCHA system, which could allow accounts to be created automatically.
Source: http://news.softpedia.com/news/Snapchat-s-Account-Registration-CAPTCHA-System-Hacked-420052.shtml

21. *January 23, The Register* – (International) **When ZOMBIES go shopping; 40m Target customer breach? That's NOTHING!** An analysis of 139 U.S. retailers between November 2013 and January 12 performed by BitSight found 1,035 instances of unique malware infections actively communicating with attackers, averaging 7.5 infections per company. The Neurevt trojan was the most common piece of malware found during the analysis, among other findings.
Source: http://www.theregister.co.uk/2014/01/23/retail_malware_epidemic/

22. *January 23, SC Magazine* – (International) **Potentially major XSS/JavaScript flaw found in Office 365.** Researchers at Cogmotive identified a vulnerability in Microsoft Office 365 that could allow a user with an organization email to use a JavaScript code to gain full administrator permissions across the organization's Office 365 environment. The vulnerability was reported to Microsoft and patched.
Source: http://www.scmagazineuk.com/potentially-major-xssjavascript-flaw-found-in-office-365/article/330685/

23. *January 23, Softpedia* – (International) **Experts spot third variant of Mac trojan used by governments in targeted attacks.** Researchers at Intego identified a new variant of the Crisis trojan that targets Mac OS X systems and has been used by governments in targeted cyberattacks.
Source: http://news.softpedia.com/news/Experts-Spot-Third-Variant-of-Mac-Trojan-

Used-by-Governments-in-Targeted-Attacks-419899.shtml

24. *January 23, Help Net Security* – (International) **Facebook awards $33,500 bounty for critical flaw.** Facebook awarded a security researcher $33,500 as part of its bug bounty program for disclosing an XML external entities (XXE) vulnerability that could be exploited to allow attackers to read arbitrary files on Facebook's servers. Source: http://www.net-security.org/secworld.php?id=16251

25. *January 23, Threatpost* – (International) **Chrome eavesdropping exploit published.** A researcher released exploit code for a vulnerability he reported in Google's Chrome browser that could allow a malicious Web site to use a computer's microphone to eavesdrop without the user being aware. Source: http://threatpost.com/chrome-eavesdropping-exploit-published/103798

26. *January 22, Softpedia* – (International) **World Economic Forum's website plagued by XSS and other security issues.** Researchers at High-Tech Bridge identified several security issues on the Web site of the World Economic Forum, including cross-site-scripting (XSS) vulnerabilities, an invalid SSL certificate, and a flaw that exposed the email addresses of individuals who had contacted the organization. Source: http://news.softpedia.com/news/World-Economic-Forum-s-Website-Plagued-by-XSS-and-Other-Security-Issues-419674.shtml

27. *January 22, Threatpost* – (International) **Small number of malicious TOR exit relays snooping on traffic.** Researchers reported in a paper that 25 exit relays in the The Onion Router (TOR) network were configured maliciously or in a way that could present a security issue. The malicious or misconfigured exit relays could allow man-in-the-middle attacks and traffic monitoring. Source: http://threatpost.com/small-number-of-malicious-tor-exit-relays-snooping-on-traffic/103771

For another story, see item **4**

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

Nothing to report

[Return to top]

Commercial Facilities Sector

28. *January 23, Altoona Mirror* – (Pennsylvania) **Fire claims J&O warehouse.** Authorities believe a short-circuit in a vintage truck may have sparked a fire at the J&O Fireplaces warehouse in Duncansville January 21. The blaze destroyed the structure, along with the machinery and more than $200,000 worth of inventory located within. Source: http://www.altoonamirror.com/page/content.detail/id/578401/Fire-claims-J-O-warehouse.html

29. *January 23, KTRK 13 Houston* – (Texas) **Two-alarm fire causes major damage at southeast Houston apartments.** One person was injured January 22 after a 2-alarm fire erupted at a Houston apartment complex, causing extensive damage to the structure and displacing the residents of 20 units. Source: http://abclocal.go.com/ktrk/story?section=news/local&id=9403929

30. *January 22, KTXL 40 Sacramento* – (California) **Explosion rocks Rancho Cordova apartment complex.** Two people were hospitalized and one firefighter was injured after a drug lab exploded at a Rancho Cordova apartment complex January 22. At least 146 residents were displaced by the explosion, which forced authorities to shut off services to the building. Source: http://fox40.com/2014/01/22/explosion-rocks-rancho-cordova-apartment-complex/

31. *January 22, The Keynoter* – (Florida) **Fire chief: Sprinkler system might have lessened Salty's damage.** A fire broke out at Salty's Waterfront Grill in Marathon and spread to the adjacent 7 Mile Marina January 22, causing an estimated $1 million in damages. The cause of the fire was under investigation. Source: http://www.keysnet.com/2014/01/22/494144/fire-chief-sprinkler-system-might.html

32. *January 22, Florida Today* – (Florida) **Pickup crashes into That Little Restaurant, Melbourne man, 49, found dead of gunshot.** Officials are investigating an incident at That Little Restaurant in Melbourne, Florida, where a pickup truck crashed into the building and investigators found the driver suffered a gunshot wound to the head. Source: http://www.floridatoday.com/article/20140122/NEWS01/301220017/Pickup-crashes-into-Little-Restaurant-Melbourne-man-49-found-dead-gunshot

33. *January 21, Argus Leader* – (South Dakota) **Co-op officials hope to reopen store at temporary location after arson destroyed store.** Investigators believe an arsonist set four fires inside the Sioux Falls Co-op Natural Foods store January 19, destroying an estimated $100,000 in equipment and inventory. Source: http://www.argusleader.com/article/20140121/NEWS/301220002/Four-separate-fires-set-Co-op-Natural-Foods

34. *January 20, Los Angeles Times* – (California) **Suspected serial arsonist arrested by Santa Monica police.** Authorities announced January 20 that a man was charged in connection with setting at least 10 fires that damaged 3 apartment complexes and a car

at an auto dealership in Santa Monica during a 10-day span that began December 30, 2013.
Source: http://www.latimes.com/local/lanow/la-me-ln-suspected-serial-arsonist-arrested-by-santa-monica-police-20140120,0,6228280.story#axzz2rEyVupz4

For an additional story, see item **11**

[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

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.