Daily Open Source Infrastructure Report
29 October 2014

Top Stories

- Eleven people were sent to an area hospital after a gas leak from a pressurized tank in a backyard that prompted the closure of Abraham Lincoln High School in Riverside, California, October 27. – *Riverside Press-Enterprise* (See item **20**)
- FireEye reported on an advanced persistent threat (APT) actor dubbed APT28 stating that the group used the Sourface downloader and Chopstick and EvilToss malware to attack governments and national and international organizations. – *The Register* (See item **23**)
- Researchers reported on an advanced persistent threat (APT) group that has used the Hikit malware family to target government agencies, law enforcement, aerospace, manufacturers, media, communications, pharmaceutical, energy, educational, and other institutions in the U.S. and several other countries since 2008. – *Softpedia* (See item **26**)
- Satellite data for the National Weather Service was restored October 23 after the agency experienced an outage that lasted for more than a day after the agency first stopped receiving weather data from a network of satellites. – *Fierce Government IT* (See item **28**)

Fast Jump Menu

Energy Sector

1. *October 27, KGW 8 Portland* – (Oregon) **Weekend storm left 140K without power, cost $11M.** Utility crews continued work October 27 to restore power to the remaining 3,800 Portland General Electric customers in Portland following a strong storm October 25 that knocked out service to 140,000 customers.
   Source: http://www.kgw.com/story/news/local/2014/10/27/wind-storm-left-140000-without-power-cost-11-million/18036039/

For another story, see item **26**

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

2. *October 27, Baltimore Sun* – (Maryland) **Calvert Cliffs nuclear plant to undergo increased federal scrutiny.** The U.S. Nuclear Regulatory Commission (NRC) stated October 27 that the Calvert Cliffs nuclear power plant in Lusby will undergo increased oversight after the NRC finalized an inspection report that found that radiation detectors on the Unit 2 steam lines were set to trigger an alarm at 100 times lower than the safety threshold, which could have caused an overreaction to low readings.
   Source: http://www.baltimoresun.com/business/bs-md-calvert-cliffs-nuclear-citation-20141027-story.html

[Return to top]

Critical Manufacturing Sector

See item **26**

[Return to top]

Defense Industrial Base Sector

See items **23** and **26**

[Return to top]

Financial Services Sector

3. *October 27, Softpedia* – (International) **Banking trojan Dridex delivered through**

Microsoft Word macros. Researchers with Palo Alto Networks found that the Dridex banking malware is being distributed via Microsoft Word documents containing malicious macros in a campaign that began October 21. The malicious documents are sent in fake invoice emails and mainly target users in the U.S.
Source: http://news.softpedia.com/news/Banking-Trojan-Dridex-Delivered-Through-Microsoft-Word-Macros-463259.shtml

For another story, see item 7

[Return to top]

Transportation Systems Sector

4. *October 28, Softpedia* – (California) **Wi-Fi hotspot name keeps airplane to London grounded in Los Angeles.** An American Airlines flight from Los Angeles International Airport to London was delayed October 26 after a passenger onboard the aircraft discovered a Wi-Fi hotspot named "Al Quida Free Terror Nettwork." The plane was taxied to a remote location of the airport and held there for 3 hours as officials investigated.
Source: http://news.softpedia.com/news/WiFi-Hotspot-Name-Keeps-Airplane-to-London-Grounded-463258.shtml

5. *October 28, Chicago Tribune* – (Indiana) **As many as 10 hurt when Chicago-bound Amtrak train hits semi.** More than 10 passengers and crew members were injured October 28 when an Amtrak passenger train en route to Chicago collided with a semi-truck north of Lafayette, Indiana. The remaining passengers continued their journey via chartered bus.
Source: http://www.chicagotribune.com/news/local/breaking/chi-amtrak-train-semi-20141028-story.html

6. *October 27, St. Cloud Times* – (Minnesota) **All roads open near Highway 10 project in Rice.** All lanes on the U.S. Highway 10 overpass at Benton County Road 2 in Rice, Minnesota, were reopened to traffic October 27 signifying the end of a major construction project that started in July 2013.
Source: http://www.sctimes.com/story/news/local/2014/10/27/roads-open-near-highway-project-rice/17995425/

7. *October 27, Securityweek* – (Delaware; New Jersey) **Attackers breach PoS systems of Delaware Ferry service.** Officials from the Delaware River and Bay Authority announced October 24 that the payment card data of customers who made purchases at Cape May-Lewes Ferry terminals and vessels in Delaware and New Jersey may have been compromised due to a possible data breach detected July 30. Customers who purchased food, beverages, and retail items between September 30, 2013 and August 7, 2014 may be affected.
Source: http://www.securityweek.com/attackers-breach-pos-systems-delaware-ferry-service

8. *October 24, Palm Springs Desert Sun* – (California) **Highway 74 open after fatal motorcycle crash.** Highway 74 in Palm Desert was shut down in both directions for almost 8 hours October 24 after a man was killed when his motorcycle collided with a truck.
Source: http://www.desertsun.com/story/news/traffic/2014/10/24/fatal-motorcycle-crash-palm-desert-74/17829765/

[Return to top]

Food and Agriculture Sector

9. *October 28, Food Safety News* – (International) **Iowa beef producer charged with falsifying halal shipments.** The owner of Cedar Rapids-based Midamar Corporation was charged according to an indictment unsealed October 24 for allegedly selling beef mislabeled as halal to Indonesia and Malaysia, falsifying export applications, money laundering, and other charges after he and other employees removed labels and replaced them with fraudulent halal-certified numbers.
Source: http://www.foodsafetynews.com/2014/10/iowa-beef-producer-charged-with-falsifying-halal-shipments

10. *October 27, U.S. Food and Drug Administration* – (National) **Chetak New York L.L.C. recalls 7 oz., 14 oz., & 28 oz. packages of "Deep Raw Cashew Pieces" because of possible health risk.** The U.S. Food and Drug Administration reported October 27 that Chetak New York LLC recalled about 11,320 packages of its Deep Raw Cashew Pieces due to possible Salmonella contamination. The affected product was packaged in 7-, 14-, and 28-ounce packages and distributed to retailers nationwide.
Source: http://www.fda.gov/Safety/Recalls/ucm420689.htm

11. *October 27, U.S. Food and Drug Administration* – (Massachusetts) **Whole Foods Market Melrose recalls Vegan Gingersnap Cookies due to mislabeling and undeclared allergens.** The U.S. Food and Drug Administration announced October 26 that Whole Foods Market issued a recall for 6-pack packages of its Vegan Gingersnap Cookies due to undeclared tree nuts, milk, soy, and egg caused by mislabeling. The affected product was produced and sold at the company's Melrose, Massachusetts store between October 23 and October 26.
Source: http://www.fda.gov/Safety/Recalls/ucm420682.htm

[Return to top]

Water and Wastewater Systems Sector

12. *October 27, Hazard Herald* – (Kentucky) **City issues boil water advisory for Combs.** The City of Hazard issued a boil water advisory to a number of Hazard Water System customers October 27 due to a water main break that may have caused bacterial contamination. The advisory will remain in effect until water samples meet acceptable standards.
Source: http://www.hazard-herald.com/news/home_top-news/150311624/City-issues-

boil-water-advisory-for-Combs

13. *October 27, Kirkland Views* – (Washington) **105,000 gallons of sewage discarded into Moss Bay by King County pump failure.** A pump failure at a Kirkland waste water pump station discharged 105,000 gallons of sewage into Moss Bay October 25 when a malfunctioning sensor failed to engage an emergency generator following a power outage at the sewage pump station due to strong winds. Health officials have closed the beach at Marina Park until further notice.
Source: http://www.kirklandviews.com/blog/2014/10/27/105000-gallons-of-sewage-discarded-into-moss-bay-by-king-county-pump-failure

For another story, see item **32**

[Return to top]

Healthcare and Public Health Sector

14. *October 28, Oakland Tribune* – (California) **Castro Valley doctor charged with long-running insurance fraud.** A surgeon who ran an orthopedic practice in Castro Valley was charged the week of October 20 for conspiring with his office manager and other employees to file fake insurance claims to six insurance companies from several medical businesses operating out of an office on the Castro Valley-Hayward border. The insurance companies suffered losses totaling at least $73,000.
Source: http://www.mercurynews.com/health/ci_26809837/castro-valley-doctor-charged-long-running-insurance-fraud

For another story, see item **26**

[Return to top]

Government Facilities Sector

15. *October 28, KSAZ 10 Phoenix* – (Arizona) **City of Phoenix under attack by hacker activists.** The City of Phoenix's Internet system was down for nearly 1 hour October 25 after hackers utilized a denial of service (DoS) attack blocking access to the city's Web site and online services while also disrupting the police department's computers. Authorities are investigating the incident and are working to secure its systems.
Source: http://www.fox10phoenix.com/story/27055272/2014/10/28/city-of-phoenix-under-attack-by-hacker-activists

16. *October 28, WMC 5 Memphis* – (Tennessee) **3 children injured in school bus accident near I-240.** Three students were transported to area hospitals after a vehicle crashed into a Durham School Services bus on an Interstate 240 overpass in Memphis October 27.
Source: http://www.wmcactionnews5.com/story/27023856/police-called-to-school-bus-accident-at-perkins-near-i-240

17. *October 27, KING 5 Seattle* – (Washington) **Student arrested for bringing homemade bomb to school.** Center School in Seattle was evacuated and classes were dismissed October 27 after a student brought a molotov cocktail to school. The device was not ignited and police arrested the teenager without incident.
Source: http://www.king5.com/story/news/local/seattle/2014/10/27/center-school-evacuation/18008487/

18. *October 27, Southern Illinoisan* – (Illinois) **Bomb threat prompts Franklin County, Ill., officials to close schools.** All Franklin County, Illinois schools were closed October 28 due to a bomb threat received by the circuit clerk's office October 27 targeting an unspecified school. Authorities are investigating the threat.
Source: http://www.stltoday.com/news/local/education/bomb-threat-prompts-franklin-county-ill-officials-to-close-schools/article_be20f417-6c4b-5d57-89d0-310a41bba045.html

19. *October 27, Newark Star-Ledger* – (New Jersey) **Howell school bus crash sends 5 students to the hospital.** An accident involving Neptune High School and Howell Middle School North buses on Route 33 in Howell October 27 caused 5 students to be transported to area hospitals with injuries after one bus rear-ended the other.
Source: http://www.nj.com/monmouth/index.ssf/2014/10/howell_school_bus_crash_sends_5_students_to_the_hospital.html

20. *October 27, Riverside Press-Enterprise* – (California) **Riverside: Gas leak sends 11 to hospital; quarantine lifted.** Eleven people were sent to an area hospital for observation following a gas leak from a pressurized tank in a backyard that prompted the closure of Abraham Lincoln High School in Riverside October 27, as well as the temporary quarantine of several blocks surrounding the tank. The containment order was lifted after authorities removed the source of the gas and sealed the leak which was caused by a corroded valve.
Source: http://www.pe.com/articles/gas-752847-school-unknown.html

21. *October 27, Reuters* – (Washington) **Washington school cancels class as community mourns shooting victims.** Marysville-Pilchuck High School north of Seattle was closed October 27 after an armed student opened fire on 5 classmates before fatally shooting himself October 24. The cafeteria on campus will remain closed while officials determine when to reopen the school.
Source: http://www.msn.com/en-us/news/us/washington-school-cancels-class-as-community-mourns-shooting-victims/ar-BBbwME1

For additional stories, see items **23**, **25**, and **26**

[Return to top]

Emergency Services Sector

22. *October 28, Mansfield News Journal* – (Ohio) **Madison teen charged with**

impersonating police officer. Authorities arrested and charged a Madison Comprehensive High School student with impersonating a peace officer after officials alleged the teenager was operating a white unmarked police cruiser with flashing lights, making up to 12 stops since October 13.
Source: http://www.mansfieldnewsjournal.com/story/news/local/2014/10/28/madison-teen-charged-impersonating-police-officer/18048371/

For additional stories, see items **15** and **26**

[Return to top]

Information Technology Sector

23. *October 28, The Register* – (International) **EvilToss and Sourface hacker crew 'likely' backed by Kremlin - FireEye.** FireEye released a report on an advanced persistent threat (APT) actor dubbed APT28 stating that the group used the Sourface downloader and Chopstick and EvilToss malware to attack NATO, Eastern European governments, European defense industry events, the World Bank, and other national and international organizations. The researchers stated that APT28 has been active since 2007 and was likely backed by the Russian government.
Source: http://www.theregister.co.uk/2014/10/28/us_mandiant_claims_moscow_sponsoring_apt_28_hacker_group/

24. *October 28, Securityweek* – (International) **Attackers exploit ShellShock via SMTP to distribute malware.** Binary Defense Systems researchers reported that attackers are leveraging the ShellShock vulnerability in GNU Bash to target servers by adding the ShellShock payload to email subject, from, and to fields, abusing the Simple Mail Transfer Protocol (SMTP). If a system is compromised, a Perl-based IRC bot is downloaded and the SMTP gateway is added to a botnet designed for distributed denial of service (DDoS) attacks.
Source: http://www.securityweek.com/attackers-exploit-shellshock-smtp-distribute-malware

25. *October 28, IDG News Service* – (International) **'ScanBox' keylogger targets Uyghurs, US think tank, hospitality industry.** Researchers at PricewaterhouseCoopers found that the ScanBox keylogging framework may be being used by several attacker groups after it was found being used to perform keylogging attacks on a variety of Web sites, including a U.S. think tank and other sites. ScanBox was first discovered in August and uses JavaScript rather than installing malware to collect keystrokes and other information.
Source: http://www.networkworld.com/article/2839600/security/scanbox-keylogger-targets-uyghurs-us-think-tank-hospitality-industry.html

26. *October 28, Softpedia* – (International) **Sophisticated Chinese espionage group after Western advanced technology.** A group of security and information technology companies coordinated by Novetta released a report into an advanced persistent threat

(APT) group dubbed Axiom Group that has used the Hikit malware family and other tools to target government agencies, law enforcement, aerospace, manufacturers, media, communications, pharmaceutical, energy, educational, and other institutions in the U.S. and several other countries since 2008. The researchers stated that the group originates in China and appears to choose targets in line with Chinese government policies.
Source: http://news.softpedia.com/news/Sophisticated-Chinese-Espionage-Group-After-Western-Advanced-Technology-463348.shtml

27. *October 27, Securityweek* – (International) **Targeted attacks against businesses jump: Kaspersky Lab.** Kaspersky Labs and B2B International released the results of a survey covering 3,900 respondents in 27 countries and found that 94 percent of businesses surveyed reported at least one cybersecurity incident in the past 12 months, with 12 percent of the countries surveyed reporting one or more targeted attack, among other findings.
Source: http://www.securityweek.com/targeted-attacks-against-businesses-jump-kaspersky-lab

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

28. *October 27, Fierce Government IT* – (Maryland) **National Weather Service suffers satellite data outage, potentially affecting forecast quality.** Satellite data for the National Weather Service was restored October 23 after the agency experienced a satellite data outage that lasted for more than a day after the agency first stopped receiving weather data from a network of satellites October 21. The agency stated that the outage could potentially affect forecast quality.
Source: http://www.fiercegovernmentit.com/story/national-weather-service-suffers-satellite-data-outage-potentially-affectin/2014-10-27

For another story, see item **26**

[Return to top]

Commercial Facilities Sector

29. *October 28, KTBC 7 Austin* – (Texas) **Apartment fire in northwest Austin.** The Keystone Apartments complex in Austin suffered an estimated $300,000 in damage from a fire that broke out October 27 and caused the displacement of several residents.

Officials determined that improperly discarded smoking material was the source of the fire.
Source: http://www.myfoxaustin.com/story/27057265/apartment-fire-in-northwest-austin

30. *October 28, Rutherford South Bergenite* – (New Jersey) **Bomb threats made against two Lyndhurst supermarkets over the weekend.** A Stop & Shop grocery store in Lyndhurst was evacuated for about 2 hours October 26 while police inspected and cleared the scene after the supermarket received a phoned bomb threat. An identical threat was called into a ShopRite store in the township, prompting an evacuation that lasted more than 2 hours while police searched and cleared the store.
Source: http://www.northjersey.com/news/crime-and-courts/bomb-threats-made-against-two-lyndhurst-supermarkets-over-the-weekend-1.1119723

31. *October 28, KTLA 5 Los Angeles* – (California) **Fire inside Taco Bell in San Bernardino prompts arson investigation.** Authorities are investigating to determine if arson was the cause of a 2-alarm fire at a Taco Bell fast food restaurant in San Bernardino October 28 that ignited after business hours.
Source: http://ktla.com/2014/10/28/fire-inside-taco-bell-in-san-bernardino-prompts-arson-investigation/

32. *October 27, KIMA 29 Yakima* – (Washington) **Crews evaluating road damage after water main break.** Several businesses in Yakima suffered water damage to their structures and merchandise after 150,000 gallons of water gushed from a water main that broke the weekend of October 25. Crews repaired the line and a stretch of Yakima Avenue was closed indefinitely due to damage and flooding.
Source: http://www.kimatv.com/news/local/Crews-evaluating-road-damage-after-water-main-break-280593132.html

33. *October 27, Associated Press* – (Nevada) **OSHA issues 2 citations for Reno Discovery Museum fire.** The Terry Lee Wells Nevada Discovery Museum in Reno was cited by the Nevada Occupational Health and Safety Administration October 27 for 2 violations and fined $2,100 following a flash fire that injured 13 people during a demonstration at the museum in September.
Source: http://www.rgj.com/story/news/2014/10/27/osha-issues-citations-discovery-reno-museum-fire/18023825/

[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