Homeland Security

Daily Open Source Infrastructure Report
01 July 2014

Top Stories

- Symantec researchers identified an ongoing, multi-phase cyberattack campaign targeting the energy sector in the U.S. and several other countries. – *Securityweek* (See item **1**)

- General Motors announced recalls June 27 covering 474,000 vehicles globally, with the largest recall affecting around 467,000 Chevrolet and GMC trucks and SUVs mainly in the U.S. and Canada. – *Associated Press* (See item **4**)

- The Alabama Department of Public Health notified over 500 people that their identities may have been stolen from department records as part of an alleged $20 million tax fraud that operated in Alabama and Georgia. – *WBMA 58 Birmingham* (See item **20**)

- Butler University in Indianapolis informed 163,000 current and past students and employees that their personal and financial information may have been compromised in a hacking incident sometime between November 2013 and May. – *WXIN 59 Indianapolis* (See item **22**)

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. *June 30, Securityweek* – (International) **Energy companies in Europe, US hit by sophisticated attack campaign.** Symantec researchers identified an ongoing cyberattack campaign by a group known as Dragonfly or Energetic Bear targeting the energy sector in the U.S. and several other countries. The campaign has used phishing emails, watering hole attacks, and a recently-uncovered compromise of several industrial control system manufacturers' Web sites.
Source: http://www.securityweek.com/energy-companies-europe-us-hit-sophisticated-attack-campaign

2. *June 28, Columbus Dispatch* – (Ohio) **Fire at natural-gas well site in Monroe County forces evacuations.** Statoil USA Onshore Properties, Inc., reported June 28 that a fire at its Eisenbarth natural gas well pad in Ohio Township was limited to the surface and was not burning in any wells. Nearby residents were evacuated while authorities investigated the incident.
Source: http://www.dispatch.com/content/stories/local/2014/06/28/natural-gas-well-fire.html

3. *June 27, WTKR 3 Hampton Roads* – (Virginia) **3,500 gallons of fuel spilled in Norfolk; Monticello Ave. reopened.** A faulty sensor on a generator caused 3,500 gallons of diesel fuel to overflow and spill on Monticello Avenue from 14th Street to 20th Street in Norfolk June 27 after the sensor mistakenly called for more fuel to be added. The roadway was closed for several hours while crews cleaned up the diesel.
Source: http://wtkr.com/2014/06/27/fuel-spill-closes-monticello-ave-from-14th-to-20th-streets/

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

See item **36**

[Return to top]

Critical Manufacturing Sector

4. *June 27, Associated Press* – (International) **GM issues 3 more recalls covering 474,000 vehicles.** General Motors announced recalls June 27 covering 474,000 vehicles globally, with the largest recall affecting around 467,000 model year 2014 and 2015

Chevrolet Silverado, Suburban, and Tahoe, and GMC Sierra and Yukon vehicles mainly in the U.S. and Canada due to a transmission software glitch that could cause the vehicles to shift into neutral on their own.
Source: http://www.wzzm13.com/story/news/2014/06/27/gm-recalling-474k-vehicles/11557881/

5. *June 27, Wilkes-Barre Citizens' Voice* – (Pennsylvania) **Cause of factory fire in Jessup under investigation.** A fire that broke out at an industrial park in Jessup June 27 destroyed the Scranton Cooperage factory and released a purple liquid believed to be paint into an adjacent wetland. The Pennsylvania Department of Environmental Protection is investigating the spill.
Source: http://citizensvoice.com/news/cause-of-factory-fire-in-jessup-under-investigation-1.1710421

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

6. *June 30, Securityweek* – (International) **"Emotet" banking malware steals data via network sniffing.** Researchers at Trend Micro identified a new piece of banking malware dubbed Emotet that attempts to steal banking credentials by logging outgoing traffic and comparing it against a list of targeted financial institutions. The malware is distributed via spam emails containing a link to a malicious Web site, and currently is primarily targeting financial institutions in Germany.
Source: http://www.securityweek.com/emotet-banking-malware-steals-data-network-sniffing

For another story, see item **20**

[Return to top]

Transportation Systems Sector

7. *June 30, Reuters* – (Kansas) **Emergency evacuation slide deploys midair on United flight.** United Airlines Flight 1463 headed to Orange County's John Wayne Airport from Chicago's O' Hare International Airport landed in Wichita, Kansas, after an emergency evacuation chute inflated inside the aircraft mid-flight June 29. Authorities are investigating the incident.
Source: http://www.huffingtonpost.com/2014/06/30/emergency-evacuation-slide-deploys_n_5542665.html

8. *June 29, KTLA 5 Los Angeles* – (California) **All lanes reopen after big rig crash shuts down 101 Freeway in Westlake Village.** Westbound lanes of the 101 Freeway in Westlake Village were closed for several hours after a semi-truck ran into the center divider and became engulfed in flames June 29. Eastbound lanes of the freeway reopened June 30 after being closed for 7 hours.
Source: http://ktla.com/2014/06/29/101-closed-in-westlake-village-after-fiery-semi-truck-crash/

9. *June 28, KSAT 12 San Antonio* – (Texas) **Man hit, killed by train on city's South Side.** Train service resumed more than 2 hours after a man was hit and killed by a freight train June 27 near San Antonio's South Side after he walked onto the tracks as the crossing arm was down and the lights were flashing.
Source: http://www.ksat.com/news/man-hit-killed-by-train-on-citys-south-side/26693712

Food and Agriculture Sector

10. *June 29, Associated Press* – (Pennsylvania) **Child dies when Italian ice shop door falls on her.** A child was fatally struck by a metal security grate that detached and fell from the facade of a Rita's Water Ice store in the Brewerytown section of Philadelphia June 28. Authorities from the Philadelphia Department of Licenses and Inspections are investigating what caused the door to fall.
Source: http://news.msn.com/us/child-dies-when-italian-ice-shop-door-falls-on-her

11. *June 27, Food Poisoning Bulletin* – (Colorado) **Hepatitis A exposure at Tortilla Marissa's in Fort Collins, CO.** Health officials warned patrons who ate or drank at Tortilla Marissa's North of the Border Cafe in Fort Collins since June 13 that they may have been exposed to hepatitis A and should receive a hepatitis A or immunoglobulin vaccination. The advisory was issued after it was confirmed that a food handler worked at the restaurant while infected with the illness.
Source: http://foodpoisoningbulletin.com/2014/hepatitis-a-exposure-at-tortilla-marissas-in-fort-collins-co/

12. *June 27, U.S. Food and Drug Administration* – (National) **Nestle USA issues recall of limited amounts of Haagen-Dazs Chocolate Chocolate Chip Ice Cream in east coast region due to mismatched packaging.** Nestle USA issued a recall for approximately 10,000, 14-ounce cartons of its Haagen-Dazs Chocolate Chocolate Chip Ice Cream due to undeclared peanuts caused by mismatched packaging. The product was produced May 13 and distributed to retailers in several States.
Source: http://www.fda.gov/Safety/Recalls/ucm403194.htm

13. *June 27, U.S. Food and Drug Administration* – (Washington) **Richard's Rubs & Seasonings recalls sauces because of possible health risk.** Richard's Rubs & Seasonings LLC issued a recall for 12-ounce bottles of its BBQ, hot, and teriyaki sauces due to the possibility they were improperly processed and may be contaminated

with Clostridium botulinum, which can cause botulism. The products were sold in grocery stores and butcher shops in western Washington.
Source: http://www.fda.gov/Safety/Recalls/ucm403200.htm

14. *June 27, U.S. Department of Agriculture* – (National) **Pennsylvania firm recalls deli ham product due to possible foreign matter contamination.** The Food Safety and Inspection Service announced June 27 that E. G. Emils & Sons, Inc., issued a recall for about 5,896 pounds of Wegman's Food You Feel Good About Organic Ham product due to possible contamination with extraneous materials. The problem was discovered by a worker at a Wegman's store and was traced to a piece of plastic that detached from an interlocker belt during production.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2014/recall-042-2014-release

[Return to top]

Water and Wastewater Systems Sector

15. *June 30, WECT 6 Wilmington* – (North Carolina) **2,000 gallons of wastewater overflow into Pages Creek.** Cape Fear Public Utility Authority crews stopped and repaired an overflow at the Country Haven Pump Station in Ogden July 27 after 2,000 gallons of wastewater flowed into Pages Creek. Health officials tested the water quality at various locations around the area and results were expected within 24 hours.
Source: http://www.wect.com/story/25896446/2000-gallons-of-wastewater-overflow-into-pages-creek

16. *June 29, Long Island Newsday* – (New York) **Bay Park sewage plant to get 18-foot-high wall and berm to protect it from storm surges.** A $37.5 million project will begin in July in Nassau County to safeguard the Bay Park Sewage Plant, which flooded during Superstorm Sandy in 2012. The project includes plans to build an earthen berm and an 18-foot-high concrete wall around the plant.
Source: http://www.newsday.com/long-island/nassau/bay-park-sewage-plant-to-get-18-foot-high-wall-and-berm-to-protect-it-from-storm-surges-1.8608855

17. *June 27, Sarasota Herald-Tribune* – (Florida) **OK to swim again at Venice Beach.** The Florida Department of Health lifted a no-swim advisory at Venice Beach June 28 when follow-up tests showed bacteria levels were back to normal after the beach was closed June 26 due to elevated enterococci bacteria levels.
Source: http://www.heraldtribune.com/article/20140627/ARTICLE/140629706/2055/NEWS?Title=UPDATE-OK-to-swim-again-at-Venice-Beach

18. *June 27, WLNE 6 New Bedford* – (Massachusetts; Rhode Island) **10,000 gallons of sewage leaked into Bristol river.** A crack in the force main valve at a pump station caused 10,000 gallons of sewage to leak into the Kickemuit River and Mount Hope Bay area in Bristol June 26. The system was repaired and a shell-fishing ban and contact recreation restrictions were announced until test results could deem the area safe.

Source: http://www.abc6.com/story/25889493/10000-gallons-of-sewage-leaked-into-bristol-river

Healthcare and Public Health Sector

19. *June309, WDSU 6 New Orleans* – (Louisiana) **Power outage at Ochsner Medical Center West Bank affects patients.** Ochsner Medical Center's West Bank campus on Belle Chasse Highway in New Orleans lost power for more than 5 hours June 28. A scheduled update to the hospital's generator lasted for more than 2 hours and hospital officials reported that no patients were ever at risk.
Source: http://www.wdsu.com/news/power-outage-at-ochsner-medical-center-affects-patients/26708664

20. *June 27, WBMA 58 Birmingham* – (Alabama; Georgia) **Alabama Department of Public Health warns patient records may have been compromised.** The Alabama Department of Public Health notified over 500 people that their identities may have been stolen from department records as part of a tax fraud scheme in which 10 people have already been indicted for allegedly using the stolen information to file over $20 million in fake tax returns in Alabama and Georgia.
Source: http://www.abc3340.com/story/25888518/alabama-department-of-public-health-warns-patient-records-may-have-been-compromised

21. *June 27, Al.com* – (Alabama) **Tuscaloosa Police arrest former hospital employee for stealing data from DCH Regional Medical Center.** The Tuscaloosa Police Department arrested a former employee June 26 in connection to stealing data from a clearing house used by DCH Regional Medical Center after files were removed June 16. The medical center is investigating and will notify any patients affected by the data download.
Source: http://www.al.com/news/tuscaloosa/index.ssf/2014/06/tuscaloosa_police_arrest_hospi.html

Government Facilities Sector

22. *June 30, WXIN 59 Indianapolis* – (Indiana; California) **Butler alumni, current and prospective students warned of data breach.** Butler University in Indianapolis informed 163,000 current and past students and employees that their personal and financial information may have been compromised in a hacking incident sometime between November 2013 and May. The university began its investigation after authorities in California arrested an individual in possession of a flash drive containing information of Butler University employees.
Source: http://fox59.com/2014/06/30/butler-university-alumni-current-students-warned-of-data-breach

23. *June 29, WFSB 3 Hartford* – (Arizona) **San Juan Fire grows to 5,700 acres.** Fire crews reached 5 percent containment June 29 of the 5,700-acre San Juan Fire burning in the Fort Apache Indian Reservation and the Apache-Sitgreaves National Forest in Vernon, Arizona. Several areas were placed under a mandatory evacuation order and about 90 structures are threatened.
Source: http://www.wfsb.com/story/25882311/san-juan-fire-explodes-to-2000-acres-in-northeast-az

[Return to top]

Emergency Services Sector

24. *June 27, Associated Press* – (Georgia) **Federal prison officials: inmate has escaped from minimum security prison work camp in Atlanta.** Federal Bureau of Prisons' officials reported that an inmate escaped from the minimum security Federal Prison Camp at the United States Penitentiary in Atlanta June 27. A search is underway and authorities advised the public to contact police if they encounter the inmate.
Source: http://www.tribtown.com/view/story/150e34dbe687457b89498da1e7b2ba7a/GA--Escaped-Inmate

25. *June 26, Salem Statesman Journal* – (Oregon) **9-1-1 service restored in north end of valley.** Frontier Communications announced June 26 that a telephone fiber was severed during road construction work near the city of Dundee prompting an outage of emergency 9-1-1 landline phone service, regular landline service, and Internet access in parts of Mid-Valley that lasted for more than 4 hours.
Source: http://www.statesmanjournal.com/story/news/2014/06/26/service-restored-north-end-valley/11429945/

[Return to top]

Information Technology Sector

26. *June 30, The Register* – (International) **London teen charged over Spamhaus mega-DDoS attacks.** Authorities in the U.K. charged a teenager for his alleged involvement in several major distributed denial of service (DDoS) attacks against anti-spam service Spamhaus during 2013. The attacks were also led to worldwide disruptions in Internet exchanges and services.
Source: http://www.theregister.co.uk/2014/06/30/ddos_charges/

27. *June 30, Threatpost* – (International) **PHP fixes OpenSSL flaws in new releases.** The PHP Group released new versions of PHP, closing two vulnerabilities in OpenSSL that are related to timestamps.
Source: http://threatpost.com/php-fixes-openssl-flaws-in-new-releases/106908

28. *June 30, Help Net Security* – (International) **Google Drive update fixes data-leaking**

flaw. Google closed a security issue in its Google Drive service that previously allowed some files shared with a direct link to be accessed by unauthorized third parties. Some files could still be seen by unauthorized parties, and Google advised users with files that met certain criteria to remove them.
Source: http://www.net-security.org/secworld.php?id=17067

For another story, see item **1**

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

See item **25**

[Return to top]

Commercial Facilities Sector

29. *June 30, Associated Press* – (California) **Dozens stranded when SeaWorld ride malfunctions.** A power failure caused the Skytower revolving capsule ride at SeaWorld San Diego to unexpectedly stop about 220 feet above the ground, stranding 46 patrons and 2 employees inside for 4 hours June 29. Firefighters were in position as a precaution until crews restored power and the ride descended to ground level without any injuries.
Source: http://news.msn.com/us/dozens-stranded-when-seaworld-ride-malfunctions

30. *June 30, KMGH 7 Denver* – (Colorado) **Firefighter hurt in 3-alarm fire at high rise in Golden.** Three residents and a firefighter were injured in a 3-alarm fire at the Ridgemoor Apartments complex in Golden June 30. Dozens of residents were evacuated from the structure while firefighters battled the blaze.
Source: http://www.thedenverchannel.com/news/local-news/fire-damages-high-rise-complex-in-golden

31. *June 29, Associated Press* – (California) **1 dead, 5 injured in awards party violence in LA.** One person was killed and 4 others were injured by gunfire at Monalizza Restaurant & Banquet Hall in Los Angeles June 29, and a fifth individual suffered non-life-threatening injuries when he was stabbed at the Lure Nightclub in Hollywood June 28. Police are searching for suspects in both incidents which took place at unsanctioned parties related to the BET Awards show.
Source: http://news.msn.com/crime-justice/1-dead-5-injured-in-awards-party-violence-

in-la

32. *June 29, Associated Press* – (Pennsylvania) **Cops: Woman shot during Pa. gun show demo.** Authorities are investigating after an employee of a vendor, In Case of Emergency Enterprises, accidentally shot a woman in the leg while demonstrating a gun and holster at the Eagle Arms Gun show at the Bloomsburg Fairgrounds in Pennsylvania June 28. The vendor believed the gun was unloaded when he demonstrated the products.
Source: http://www.usatoday.com/story/news/nation/2014/06/29/gun-show-accident/11724435/

33. *June 27, WZZM 13 Grand Rapids* – (Michigan) **Arson not suspected in Alpine Ave. blaze.** Firefighters decided to stop using water and let a fire at Fox Pools in Alpine Township burn June 25 to minimize potential environmental damage, including ground water contamination, due to the amount of hazardous pool chemicals stored at the facility. Authorities are investigating the cause of the fire.
Source: http://www.wzzm13.com/story/news/local/metro/2014/06/25/fox-pools-alpine-township-fire/11350781/

34. *June 27, KTVK 3 Phoenix* – (Arizona) **Dozens displaced by west Phoenix apartment fire.** A June 27 fire at the San Marina Apartments complex in west Phoenix displaced up to 60 people and damaged the entire structure.
Source: http://www.azfamily.com/news/Dozens-displaced-by-west-Phoenix-apartment-fire-264992061.html

35. *June 26, KOCO 5 Oklahoma City* – (Oklahoma) **2 grenades found at Oklahoma City Goodwill.** A Goodwill in Oklahoma City was evacuated for 3 hours June 26 after one grenade was found inside a desk and a second grenade was found inside a warehouse on the property. Police used a robot to disable the devices without incident and declared the scene safe.
Source: http://www.koco.com/news/crews-investigating-possible-explosive-device-at-oklahoma-city-goodwill/26675590

36. *June 26, St. Louis Post-Dispatch* – (Missouri) **EPA: No public health risk from radiation at Bridgeton sports complex.** The U.S. Environmental Protection Agency announced June 26 that the Bridgeton Municipal Athletic Complex in Missouri is suitable for public use following radiation testing that showed no hazardous levels of gamma radiation at the site. The screening analyzed 58,000 surface points at the 70-acre sports complex in May and was initiated due to residents' concerns about its proximity to West Lake Landfill, where nuclear waste was illegally dumped in the 1970s.
Source: http://www.stltoday.com/lifestyles/health-med-fit/health/epa-no-public-health-risk-from-radiation-at-bridgeton-sports/article_71c7d19a-339e-5bcc-973a-44386f574fb8.html

Dams Sector

37. *June 27, Highland Community News* – (California) **Board allocates $5 million for Lake Gregory Dam repairs.** The San Bernardino County Board of Supervisors approved June 17 an additional $5 million to repair the earthen dam at Lake Gregory Regional Park, bringing the total budget to $9 million for repairs to address issues with the dam after deficiencies and issues were found.
Source: http://www.highlandnews.net/entertainment/article_cdeb2f5e-fe52-11e3-b11c-001a4bcf887a.html

For another story, see item **16**

[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.