Daily Open Source Infrastructure Report
11 June 2014

Top Stories

- Researchers at CrowdStrike released a report on a cyberespionage group dubbed Putter Panda that possibly has ties to the Chinese People's Liberation Army and primarily targets U.S, Japanese, and European aerospace, satellite, and communications industries. – *Securityweek* (See item **5**)

- A fire broke out at Sorenson Farms in Grandview, Washington, June 8 which caused an estimated $1.5 million in damage. – *Yakima Herald-Republic* (See item **13**)

- Firefighters reached 65 percent containment on a fire that broke out June 9 at a Thompson Hardwoods wood processing facility in Hazlehurst, New York, when a load of lumber was pulled out of a drying kin and strong winds spread embers from that load to other lumber in the warehouse. – *WALB 10 Albany* (See item **14**)

- Authorities are investigating the source of a Salmonellosis outbreak linked to Proper Restaurant in Boone, North Carolina, that sickened at least 37 individuals as of June 9. – *Wautauga Democrat* (See item **16**)

Fast Jump Menu

Energy Sector

1. *June 10, Bucks County Courier Times* – (Pennsylvania) **PECO has restored power after 30,000 knocked out.** PECO Energy Company restored power to about 31,000 customers in Central and Upper Bucks County June 9 after a piece of equipment at a substation malfunctioned.
Source: http://www.buckscountycouriertimes.com/news/local/more-than-without-power-in-bucks-county/article_0d716dc6-a28f-579f-bc79-7a44ee7fa70b.html

2. *June 9, KITV 4 Honolulu* – (Hawaii) **HECO: 65,000 Oahu customers affected by outage.** Crews restored service to about 65,000 Hawaiian Electric Company customers in Oahu June 9 after a generator for an independent power producer at Campbell Industrial Park, AES Corp., went offline prompting the utility's computer systems to automatically and systematically begin shutting down power to avoid an island-wide outage. Officials are investigating the cause of the outage.
Source: http://www.kitv.com/news/heco-tens-of-thousands-may-be-affected-by-oahu-outage/26407976

[[Return to top]]

Chemical Industry Sector

Nothing to report

[[Return to top]]

Nuclear Reactors, Materials, and Waste Sector

3. *June 10, Nuclear Street* – (Illinois) **Dresden excavates area near tank after tritium leak.** The operators of the Dresden nuclear power plant in Illinois stated June 9 that crews were working to secure a leak of water containing tritium at 1.3 million picocuries per liter (pCi/L), above the 1 million pCi/L release limit, after a leak was detected in a water storage tank June 7. Crews were working to excavate the area near the tank and to identify and repair the leak.
Source:http://nuclearstreet.com/nuclear_power_industry_news/b/nuclear_power_news/archive/2014/06/10/dresden-excavates-area-near-tank-after-tritium-leak-061001.aspx

[[Return to top]]

Critical Manufacturing Sector

See item **4**

[[Return to top]]

Defense Industrial Base Sector

4. *June 10, Securityweek* – (International) **Cyber spies targeting U.S. defense, tech firms linked to China's PLA: Report.** Researchers at CrowdStrike released a report on a cyberespionage group dubbed Putter Panda that has primarily targeted U.S, Japanese, and European aerospace, satellite, and communications industries and appears to be tied to the Chinese People's Liberation Army's Unit 61486. The group has been active since at least 2007 and mostly relies on custom malware that exploits vulnerabilities in popular software, according to the report. Source: http://www.securityweek.com/cyber-spies-targeting-us-defense-tech-firms-linked-chinas-pla-report

Financial Services Sector

5. *June 10, Securityweek* – (International) **Zeus alternative "Pandemiya" emerges in cybercrime underground.** Researchers with RSA identified a completely new banking trojan known as Pandemiya that has several typical banking fraud tools as well as a modular design. The trojan does not share any code in common with other banking fraud toolkits and has appeared for sale on underweb marketplaces. Source: http://www.securityweek.com/zeus-alternative-pandemiya-emerges-cybercrime-underground

6. *June 9, Orlando Sentinel* – (Florida) **Feds charge Longwood man in $76 million fraud scheme.** Federal authorities announced June 9 that a Longwood man who operated United Credit Recovery was arrested on charges that he allegedly ran the company as a $76 million fraud and bribery scheme. Authorities allege that the man would forge documentation from banks on overdraft debt in order to sell the debt as debt of a higher quality, and that he also paid over $1 million in bribes to a U.S. Bank official to obtain insider information. Source: http://www.orlandosentinel.com/news/local/breakingnews/os-united-credit-recovery-fraud-scheme-20140609,0,2404997.story

7. *June 9, U.S. Attorney's Office, Eastern District of New York* – (New York) **Fund manager arrested and charged in $17 million Ponzi scheme.** A St. James, New York fund manager was arrested and charged June 9 for allegedly running a $17 million Ponzi scheme that operated between January 2000 and June 2009 and raised funds from at least 74 investors. Source: http://www.fbi.gov/newyork/press-releases/2014/fund-manager-arrested-and-charged-in-17-million-ponzi-scheme

For another story, see item **27**

Transportation Systems Sector

8. *June 10, KMGH 7 Denver* – (Colorado) **Huge house fire closed Highway 83 south of Franktown.** Highway 83 in Douglas County, Colorado, was shut down overnight June 9-10 after a fire destroyed a home in Franktown. No injuries were reported.
Source: http://www.thedenverchannel.com/news/huge-house-fire-closes-highway-83-south-of-franktown

9. *June 10, CNN* – (Massachusetts) **Southwest aircraft hits parked JetBlue plane.** A Southwest Airlines aircraft was taken out of service for repairs after it collided with a parked JetBlue plane while it was moving on the ground at Boston Logan International Airport June 9, causing flight delays for both airlines.
Source: http://www.wtsp.com/story/news/2014/06/10/southwest-aircraft-hits-parked-jetblue-plane/10269997/

10. *June 9, Associated Press* – (New York) **Groundbreaking for new Niagara Falls train station; last phase of $41M transportation project.** State officials were in Niagara Falls, New York, June 9 for the groundbreaking of the city's International Railway Station and Intermodal Transportation Center's third and final phase of the $41 million project. Construction is estimated to take 18-24 months and will include a new Amtrak passenger station.
Source: http://www.therepublic.com/view/story/b6c10c5598fc4de6bfb18ca8e97c8070/NY--Niagara-Falls-Amtrak-Station

11. *June 9, WLWT 5 Cincinnati* – (Ohio) **2 hospitalized after fiery multi-car accident on I-75.** Interstate 75 at State Route 129 in Liberty Township, Ohio, was closed for about 6 hours after a northbound semi-truck lost control, flipped over the center median onto southbound lanes, and caught fire. Three other cars were involved in the accident and two individuals were transported to area hospitals for injuries.
Source: http://www.wlwt.com/news/2-hospitalized-after-fiery-multi-car-accident-on-I-75/26404246

12. *June 9, KBOI 9 Boise* – (Idaho) **Woman, boy killed in Highway 55 crash near Smiths Ferry.** Highway 55 near Smiths Ferry was closed for about 2 hours June 9 after a 2-vehicle accident that killed 2 people and left 4 others injured.
Source: http://www.kboi2.com/news/local/Woman-boy-killed-in-Highway-55-crash-near-Smiths-Ferry-262436441.html

[Return to top]

Food and Agriculture Sector

13. *June 10, Yakima Herald-Republic* – (Washington) **Grandview farm shop fire racks up estimated loss topping $1M.** A fire broke out at Sorenson Farms in Grandview June 8 and engulfed a shop that was used as a small office and to store a variety of equipment, including tractors, grape pickers, forklifts, and tools. Authorities are investigating the source of the fire which caused an estimated $1.5 million in damage.
Source: http://www.yakimaherald.com/news/latestlocalnews/2247451-8/fire-destroys-

farm-shop-east-of-grandview

14. *June 9, WALB 10 Albany* – (Georgia) **Hazlehurst lumberyard burns on; economic damage enormous.** Firefighters reached 65 percent containment on a fire that broke out June 9 at a Thompson Hardwoods wood processing facility in Hazlehurst when a load of lumber was pulled out of a drying kin and strong winds spread embers from that load to other lumber in the warehouse. An office building and a warehouse, including the lumber contained within, were also destroyed by the fire.
Source: http://www.walb.com/story/25727565/hazlehurst-lumberyard-burns-on-helicopter-enroute

15. *June 9, WAPT 16 Jackson* – (Mississippi) **Richland business evacuated after ammonia leak.** Crews began efforts June 10 to release ammonia trapped inside the Millard Refrigerated Services facility in Richland following a leak that prompted an evacuation of the plant June 9. A ruptured ammonia tank in a refrigeration unit at the facility was repaired and a contractor was hired to monitor air quality outside the building.
Source: http://www.wapt.com/news/central-mississippi/richland-business-evacuated-after-ammonia-leak/26405526

16. *June 9, Watauga Democrat* – (North Carolina) **37 report Salmonellosis symptoms.** Authorities are investigating the source of a Salmonellosis outbreak linked to Proper Restaurant in Boone, North Carolina, that sickened at least 37 individuals as of June 9.
Source: http://www2.wataugademocrat.com/News/story/UPDATE-Health-department-37-report-Salmonellosis-symptoms-id-015223

17. *June 9, U.S. Department of Labor* – (Massachusetts) **US Department of Labor's OSHA cites Massachusetts seafood processor for serious safety violations following worker's death.** The Occupational Safety and Health Administration cited Sea Watch International Ltd., for seven serious workplace safety violations following an investigation prompted by a worker fatality at the company's New Bedford facility in January. Proposed penalties totaled $35,410.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=26178

18. *June 8, Food Safety News* – (National) **304 containers of Trader Joe's Egg White Salad with Chives recalled for possible Listeria.** Lansal Inc., doing business as Hot Mama's Foods, announced a recall of 304 6-ounce plastic containers of Trader Joe's Egg White Salad with Chives due to possible Listeria monocytogenes contamination.
Source: http://www.foodsafetynews.com/2014/06/trader-joes-egg-white-salad-with-chives-recalled-for-possible-listeria-contamination

19. *June 8, U.S. Food and Drug Administration* – (Texas) **Dole Packaged Foods recalls Roasted Garlic Tomato Basil Soup in Texas due to undeclared milk allergen.** Dole Packaged Foods, LLC issued a recall for 26-ounce cartons of its Dole Garden Soup

Roasted Garlic Tomato Basil that were distributed to Texas retail grocery stores due to undeclared milk.
Source: http://www.fda.gov/Safety/Recalls/ucm400259.htm

For another story, see item **33**

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

20. *June 9, Hartford Business* – (Connecticut) **400 patients' data may be compromised in Access Health breach.** Access Health CT, Connecticut's health insurance exchange reported that an employee from its call center vendor Maximus dropped a backpack June 6 in Hartford containing notepads with the personal information of about 400 health insurance customers. The backpack was found and the employee was placed on leave while officials investigate the incident.
Source: http://www.hartfordbusiness.com/article/20140609/NEWS01/140609922

For another story, see item **24**

Government Facilities Sector

21. *June 10, WATD 95.9 FM Marshfield* – (Massachusetts) **Middleboro: Minor injuries reported in school bus accident.** Eight elementary students and the bus driver were injured when their school bus was rear-ended by another vehicle in Middlesboro June 10.
Source: http://959watd.com/blog/2014/06/middleboro-minor-injuries-reported-in-school-bus-accident/

22. *June 9, Los Angeles Times* – (California) **School lockdowns lifted near North Hollywood standoff.** Several schools in North Hollywood were evacuated or placed on lockdown for several hours June 9 after a suspect armed with an assault rifle led police officers on a high-speed chase and roamed around neighborhoods before barricading himself inside a home. Police took the suspect into custody without incident.
Source: http://www.latimes.com/local/lanow/la-me-ln-valley-schools-on-lockdown-20140609-story.html

23. *June 9, Fresno Bee* – (California) **6 Central Unified students receive minor injuries in bus collision.** An accident between a Central Unified School District bus and a truck

left 6 students injured when the two vehicles collided near Fresno June 9.
Source: http://www.mercedsunstar.com/2014/06/09/3689819/central-unified-school-bus-in.html

24. *June 7, WTKR 3 Norfolk* – (Virginia) **Man accused of stabbing near Naval Medical Center Portsmouth now in custody; victim remains critical.** Authorities arrested a U.S. Navy sailor accused of stabbing another sailor near Naval Medical Center Portsmouth at Naval Support Activity Hampton Roads' Portsmouth Annex June 6. The suspect led officers on a nearly 9-hour manhunt that forced the closure of the installation and prompted a shelter in place order for the hospital.
Source: http://wtkr.com/2014/06/06/active-shooter-alert-issued-at-portsmouth-naval-medical-center/

[Return to top]

Emergency Services Sector

Nothing to report

[Return to top]

Information Technology Sector

25. *June 10, V3.co.uk* – (International) **Clandestine Fox hackers spreading malware via Facebook, Twitter and LinkedIn.** FireEye researchers detected a new attack campaign by a group known as Clandestine Fox which uses malicious attachments in social media and email messages to spread malware. The attackers behind the campaign previously utilized a vulnerability that affected multiple versions of Internet Explorer before a patch was issued by Microsoft.
Source: http://www.v3.co.uk/v3-uk/news/2349226/clandestine-fox-hackers-spreading-malware-via-facebook-twitter-and-linkedin

26. *June 9, Threatpost* – (International) **'Red button' attack could compromise some smart TVs.** Researchers with Columbia University's Network Security Lab reported that a vulnerability in the Hybrid Broadcast Broadband Television (HbbTV) feature in some smart TVs could allow attackers to steal personal information, access home networks, and perform denial of service (DoS) attacks by luring users to a compromised channel.
Source: http://threatpost.com/red-button-attack-could-compromise-some-smart-tvs/106547

27. *June 9, Securityweek* – (International) **Zeus malware control panel vulnerable: Websense.** Websense researchers published information and a proof-of-concept that illustrate how the control panel for the Zeus banking trojan can be compromised by uploading a customized file to the command and control server.

Source: http://www.securityweek.com/zeus-malware-control-panel-vulnerable-websense

28. *June 9, Securityweek* – (International) **Majority of comment spam generated by small number of attackers: Imperva.** Imperva released their June Hacker Intelligence Initiative report, which found that during the report's 2-week survey period in September 2013, 28 percent of attack sources generated 80 percent of traffic associated with comment spam, among other findings.
Source: http://www.securityweek.com/majority-comment-spam-generated-small-number-attackers-imperva

29. *June 9, SC Magazine* – (International) **Possibly 350K ransomware infections, $70K earned, in Dropbox phishing scheme.** Researchers with PhishMe found that an ongoing phishing campaign utilizing links to Dropbox may have infected almost 350,000 systems with the Cryptowall ransomware, bringing in over $70,000 in Bitcoins of ransom for the attackers.
Source: http://www.scmagazine.com/possibly-350k-ransomware-infections-70k-earned-in-dropbox-phishing-scheme/article/353559/

For additional stories, see items **4** and **5**

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

See item **4**

Commercial Facilities Sector

30. *June 10, Reuters* – (California) **Falling dolphin statue kills toddler on San Francisco vacation.** A San Francisco business was cited by police for displaying its property in an undesignated space of a sidewalk in the city's Fisherman's Wharf district after a child was fatally injured June 9 when a large metal statue toppled and struck the individual.
Source: http://news.msn.com/us/falling-dolphin-statue-kills-toddler-on-san-francisco-vacation

31. *June 10, WTSP 10 St. Petersburg* – (Florida) **Lightning cause of Carrollwood condo**

fire. Lightning struck the Grande Oasis Condos building in Carrollwood and sparked a 2-alarm structure fire that damaged 18 units and caused more than $800,000 in damage June 9. Fifty residents were displaced by the incident.
Source: http://www.wtsp.com/story/news/local/hillsboroughcounty/2014/06/09/fire-hillsborough-county-key-royale/10247997/

32. *June 9, WAFF 48 Huntsville* – (Alabama) **City condemns Huntsville apartment building.** A 20-unit building at the Continental Apartments complex in Huntsville was condemned by city officials June 9 due to concerns that the structure may collapse. Officials inspected the building after a resident notified authorities of water leaking into the electrical system following recent storms that removed a portion of the roof.
Source: http://www.waff.com/story/25729317/city-condemns-huntsville-apartment-building

33. *June 9, Easton Express Times* – (Pennsylvania) **Northampton standoff suspect captured; he demanded pizza and cash, police say.** Police took a man into custody June 9 following a 6-hour standoff that began when he claimed to have a homemade bomb attached to his apartment door located beneath the Gin Mill and Grille in Northampton. The building was evacuated and a 1-block area was cordoned off until police captured the man.
Source: http://www.lehighvalleylive.com/northampton-county/index.ssf/2014/06/northampton_standoff_suspect_c.html

34. *June 9, Associated Press* – (Colorado) **Minor injury, damage reported as eight tornadoes strike Colorado.** A storm system that produced eight tornadoes moved through Colorado June 8, damaging an office trailer at Blackstone Country Club in Aurora and injuring one person that was attending a tournament at the club. Another tornado near Lake George caused substantial damage to a recreational vehicle park.
Source: http://www.foxnews.com/weather/2014/06/09/severe-storms-slam-parts-colorado/

35. *June 8, San Antonio Express-News* – (Texas) **Texas apartment fire displaces 20.** Firefighters responded to the Auburn Creek Apartments in San Antonio June 7 due to a 2-alarm fire that broke out as a result of a resident overheating oil while cooking. The fire caused an estimated $180,000 in damages and displaced 20 residents.
Source: http://www.firehouse.com/news/11512837/two-alarm-fire-strikes-san-antonio-apartment-building

[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.