Daily Open Source Infrastructure Report
13 June 2016

Top Stories

- Two men were charged June 9 for their roles in a $250,000 bank heist and mail fraud scheme where the duo deposited over 300 altered U.S. Postal Service Money Orders into accounts at 14 banks in New York and New Jersey and later withdrew the money, causing the banks over $300,000 in losses. – *Lower Hudson Valley Journal News* (See item **2**)
- The governor of New York announced June 9 that the State will begin a $17 million project to restore and improve Niagara Falls State Park. – *Associated Press* (See item **16**)
- Multiple security firms detected that the Caliphate Cyber Army (CCA) leaked the personal information of more than 800 employees from the Arkansas Library Association (ALA) via a Structured Query Language (SQL) injection attack. – *Softpedia* (See item **21**)
- Trihedral Engineering released updates for its VTScada products used in the water, energy, nuclear, and transportation sectors, among others after discovering three critical and high severity vulnerabilities in the Wireless Application Protocol (WAP) component that can be exploited by a remote attacker. – *SecurityWeek* (See item **22**)

Fast Jump Menu

Energy Sector

1. *June 9, WYMT 57 Hazard* – (Kentucky) **State regulators cite Harlan County coal mine after sediment leaks into creek.** The Kentucky Department of Natural Resources cited Revelation Energy LLC and partially shut down operations at a Harlan County coal mine June 8 after sediment leaked into creek waters near California Hollow in the Coldiron community. State regulators ordered all mining activity on Permit 8480346 to cease until the ponds that leaked the sediment are fixed and comply with department standards.
   Source: http://www.wymt.com/content/news/State-regulators-cite-Harlan-County-coal-mine-after-sediment-leaks-into-creek-382317501.html

For another story, see item **22**

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

See item **22**

Critical Manufacturing Sector

See item **22**

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

2. *June 10, Lower Hudson Valley Journal News* – (New York; New Jersey) **2 Rockland men indicted for bank theft, mail fraud.** Two Rockland residents were charged June 9 for their roles in a $250,000 bank heist and mail fraud scheme where the duo deposited over 300 altered U.S. Postal Service Money Orders into accounts at 14 banks in Rockland and Orange counties in New York, and Bergen County in New Jersey and later withdrew the money, causing the banks more than $300,000 in losses. Officials stated the pair photocopied dollar amounts onto the fraudulent money orders, and used debit cards and personal identification numbers (PINs) linked to other individuals' bank accounts to deposit the money orders into the bank accounts via an ATM.
   Source: http://www.lohud.com/story/news/crime/2016/06/10/rockland-bank-theft/85677536/

3. *June 9, South Florida Sun-Sentinel* – (Florida) **'Filter Bandit' may have struck in Broward again, FBI says.** Authorities offered a reward June 9 in exchange for information on a man dubbed the "Filter Bandit" who is suspected of robbing a

SunTrust Bank branch in Coral Springs, Florida, June 8 and nine other banks in Broward County since August 2014. The suspect is considered armed and dangerous.
Source: http://www.sun-sentinel.com/news/crime/fl-coral-springs-filter-bandit-fbi-20160609-story.html

4. *June 9, St. Louis Post-Dispatch* – (Missouri) **Ladue arrest leads to guilty plea to fake credit card scheme.** A Bellevue, Washington man pleaded guilty June 9 to possessing over 100 fraudulent credit cards and a device to encode the cards' magnetic strips, and admitted to organizing a multi-state trip to use the fake cards after he was arrested in March in Ladue, Missouri, when authorities discovered the illicit materials.
Source: http://www.stltoday.com/news/local/crime-and-courts/ladue-arrest-leads-to-guilty-plea-to-fake-credit-card/article_360db35b-ce57-5197-b637-8e2f3d7a88f9.html

Transportation Systems Sector

5. *June 9, Victor Valley News* – (California) **1 dead, 3 injured in Highway 395 crash.** Highway 395 in San Bernardino was closed for more than 3 hours June 9 due to a head-on crash that killed one person and left three others injured. Two of the injured were sent to area hospitals for life-threatening injuries.
Source: http://www.vvng.com/1-dead-3-injured-in-highway-395-crash/

6. *June 9, WXII 12 Winston-Salem* – (North Carolina) **Motorcyclist killed in Winston-Salem crash that closed Highway 158 for hours.** A three-vehicle crash involving a motorcycle and two other vehicles resulted in the death of the motorcyclist and prompted the shutdown of Highway 158 in Winston-Salem for more than 6 hours June 9.
Source: http://www.wxii12.com/news/winstonsalem-police-crash-to-close-highway-158-for-several-hours/39980206

7. *June 9, KSFY 13 Sioux Falls* – (South Dakota) **No reports of chemical leaks in Tulare train derailment.** Two unrelated train derailments occurred June 9 involving two different BNSF Railway trains in South Dakota where nine cars derailed in northeast South Dakota and seven cars derailed in Aberdeen. No injuries or spills were reported.
Source: http://www.ksfy.com/content/news/Train-carrying-chemicals-derails-near-Tulare-382433651.html

8. *June 8, Associated Press* – (Nevada) **Southwest Airlines flight to St. Louis returns to Las Vegas.** Southwest Airlines Flight 511 en route to St. Louis from Las Vegas June 8 returned to McCarran International Airport mid-flight as a precaution to check whether the aircraft had tire and tail damage. The plane was checked by maintenance crews and was cleared to resume its flight after no problems were discovered.
Source: http://www.fireengineering.com/ap-news/2016/06/08/southwest-plane-to-st-louis-calls-emergency-lands-in-vegas.html

For additional stories, see items **15** and **22**

Food and Agriculture Sector

9. *June 10, KCRA 3 Sacramento* – (California) **Foodborne illness may be linked to Fairfield restaurant.** Alejandro's Taqueria in Fairfield, California, was shut down until further notice June 8 while health officials investigate an outbreak of Campylobacter that sickened at least 32 people after they dined at the restaurant between May 26 and May 28. Authorities collected samples of cooked food to determine the source of the outbreak.
Source: http://www.kcra.com/news/foodborne-illness-may-be-linked-to-fairfield-restaurant/39990722

10. *June 9, U.S. Food and Drug Administration* – (National) **Hershey issues voluntary recall of SoFit products due to expanded supplier recall of sunflower seeds.** The Hershey Company issued a voluntary recall June 6 for its SoFit Protein Plus Sunflower Seeds Sea Salt, SoFit Protien Plus Pumpkin Seeds Sesame Garlic, and SoFit Protein Plus Almonds Jalapeno Garlic products after the company's sunflower seed supplier, SunOpta, Inc., expanded a recall for the seeds used in the products due to potential Listeria monocytogenes contamination. No illnesses have been reported.
Source: http://www.fda.gov/Safety/Recalls/ucm506038.htm

11. *June 9, U.S. Food and Drug Administration* – (New York; New Jersey) **Fal Foods USA Inc., issues allergy alert on undeclared milk in DF Mavens Chocolate Almond Fudge Frozen Bars.** Fal Foods USA, Inc., issued a voluntary recall June 9 for one lot of its DF Mavens brand Chocolate Almond Fudge Frozen Bars products due to mislabeling and undeclared milk after the company received one consumer report of illness in connection with the undeclared milk, and Federal sampling and analysis confirmed the presence of milk in the product. The products were distributed to New York and New Jersey.
Source: http://www.fda.gov/Safety/Recalls/ucm506074.htm

12. *June 9, Associated Press* – (California) **15 hospitalized after chemical spill at food factory.** Fifteen employees at the Starkist Foods Inc., canning facility in Eastvale, California, were hospitalized June 9 due to inhalation problems after a forklift loading a concentrated cleaning acid onto a dock pierced a container, causing approximately 40 gallons of the chemical to spill. Crews worked for 3 hours containing the spill.
Source: http://www.sacbee.com/latest-news/article82934882.html

For another story, see item **22**

Water and Wastewater Systems Sector

13. *June 9, KCRG 9 Cedar Rapids* – (Iowa) **High amounts of E. coli tested at Backbone State Park**. The Iowa Department of Natural Resources issued an advisory against swimming at Backbone State Park June 9 after recent water samples showed E. coli bacteria levels exceeded the acceptable limit in the water.
Source: http://www.kcrg.com/content/news/High-amounts-of-E-Coli-tested-at-Backbone-State-Park--382417831.html

For another story, see item **22**

Healthcare and Public Health Sector

14. *June 9, Newport News Daily Press* – (Virginia) **Riverside Health System patient records may have been compromised, official says.** A spokesperson for Riverside Health System in Virginia reported June 9 that an employee who was authorized to bring patient documents home to be coded, did not immediately return 578 patient records. The health system does not believe that the paperwork containing personal and medical information was further disclosed or used inappropriately.
Source: http://www.dailypress.com/health/dp-riverside-health-system-patient-records-may-have-been-compromised-official-says-20160609-story.html

Government Facilities Sector

15. *June 10, KVOA 4 Tucson* – (Arizona) **Yarnell homes continue to be evacuated as fire grows to 5,000 acres.** Crews reached 10 percent containment June 10 of the 5,000-acre Tenderfoot Fire burning on the east side of a hill near State Route 89 in Arizona. Three structures were burned in the fire and State Route 89 into Yarnell remained closed.
Source: http://www.kvoa.com/story/32189689/yarnell-homes-continue-to-be-evacuated-as-fire-grows-to-1300-acres

16. *June 9, Associated Press* – (New York) **Niagara Falls State Park to get $17M upgrade.** The governor of New York announced June 9 that the State will rename Robert Moses Parkway the Niagara State Parkway as part of a $17 million upgrade to Niagara Falls State Park, which will include a series of updates designed to restore and improve the park.
Source: http://www.travelweekly.com/North-America-Travel/Niagara-Falls-State-Park-gets-17-million-dollar-upgrade-AP

17. *June 9, Chicago Tribune* – (Illinois) **CPS says high lead levels found at 11 more schools.** Chicago Public Schools announced June 8 that expanded lead testing to all schools in the district found high levels of lead in water at an additional 11 elementary schools, prompting authorities to shut down potable water fixtures and supply water coolers. The district is awaiting results from other buildings that were tested.
Source: http://www.chicagotribune.com/news/local/breaking/ct-cps-lead-testing-results-met-20160608-story.html

Emergency Services Sector

Nothing to report

Information Technology Sector

18. *June 10, SecurityWeek* – (International) **VMware patches critical flaw in NSX, vCNS products.** VMware released updates for its NSX Edge 6.1, 6.2, and vCloud

Networking and Security (vCNS) Edge 5.5., patching a critical input validation flaw after a company security researcher found the product contained a stored cross-site scripting (XSS) vulnerability that could allow an attacker to hijack an authenticated user's session. The company advised its users to update the products to the latest versions.
Source: http://www.securityweek.com/vmware-patches-critical-flaw-nsx-vcns-products

19. *June 10, IDG News Service* – (International) **New Mozilla fund will pay for security audits of open-source code.** Mozilla reported that it will set up a $500,000 fund, titled Secure Open Source (SOS), to pay for professional security companies to audit project code in several of its software products after the company discovered 43 flaws including a HeartBleed and Shellshock malware, a critical vulnerability, and two other flaws in its open-source products.
Source: http://www.computerworld.com/article/3082046/security/new-mozilla-fund-will-pay-for-security-audits-of-open-source-code.html#tk.rss_security

20. *June 10, Softpedia* – (International) **Crysis ransomware appears out of thin air to take TeslaCrypt's place.** Security researchers reported that the malware, Crysis could be the next TeslaCrypt malware after discovering that Crysis encrypts all contacted files, with the exception of its own binaries and core Windows files, communicates with its Command and Control (C&C) server, sends local computer details to help identify the victim, and sends information on the number of files it encrypts.
Source: http://news.softpedia.com/news/crysis-ransomware-appears-from-thin-air-to-take-teslacrypt-s-place-505082.shtml

21. *June 10, Softpedia* – (International) **ISIS hackers leak details from Arkansas Library Association.** The FBI and several other security firms detected that the Caliphate Cyber Army (CCA), an Islamic State de-facto hacking division, leaked the personal information including names, addresses, and telephone numbers of more than 800 employees from the Arkansas Library Association (ALA) by using a Structured Query Language (SQL) injection attack.
Source: http://news.softpedia.com/news/isis-hackers-leak-details-from-arkansas-library-association-505074.shtml

22. *June 9, SecurityWeek* – (International) **Trihedral patches flaws in SCADA software.** Trihedral Engineering released version 11.2.02 for its VTScada products used in the water, energy, food and agriculture, critical manufacturing, communications, nuclear, and transportation sectors after discovering three critical and high severity vulnerabilities in the Wireless Application Protocol (WAP) component including an out of-bounds read issue, a path traversal flaw, and an authentication bypass flaw that can all be exploited by a remote attacker.
Source: http://www.securityweek.com/trihedral-patches-flaws-scada-software

For another story, see item **23**

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 **22**

Commercial Facilities Sector

23. *June 10, SecurityWeek* – (International) **Wendy's finds more PoS systems hit by malware.** Wendy's fast food restaurant reported June 9 that the number of locations affected by a point-of-sale (PoS) breach was much higher than previously anticipated after an investigation revealed unrelated cybersecurity issues had been identified at approximately 300 other franchise restaurants following the infection of a remote access tool (RAT) that was found on PoS systems. Officials are continuing to investigate the incident and the food chain did not give an exact number of affected locations.
Source: http://www.securityweek.com/wendys-finds-more-pos-systems-hit-malware

24. *June 9, Santa Fe New Mexican* – (New Mexico) **Bomb scare prompts evacuations at Santa Fe apartment complex.** Santa Fe police reported June 9 that a phoned bomb threat prompted an evacuation for part of the Avaria of Santa Fe apartment complex for about 2 hours June 8 after a man claimed he had taken a hostage and had several pipe bombs. A bomb squad searched the building for any explosive devices, but no dangerous materials were found.
Source: http://www.santafenewmexican.com/news/local_news/bomb-scare-prompts-evacuations-at-santa-fe-apartment-complex/article_52967aef-598e-5358-8f9f-7a4cb2245bc0.html

Dams Sector

Nothing to report

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