Daily Open Source Infrastructure Report
29 June 2015

Top Stories

- The Boise Police Department's Organized Retail Crime Unit in Idaho arrested 2 suspects June 24 and seized 424 counterfeit credit and gift cards along with merchandise that they had bought with the fraudulent cards. – *Boise Weekly* (See item **8**)

- Interstate 75 in Chattanooga, Tennessee, reopened June 26 after being closed for about 12 hours due to a 9-vehicle accident that killed 6 people June 25. – *Associated Press* (See item **9**)

- The California Assembly passed a bill June 25 restricting exemptions for mandatory vaccination schedules, negating the State's personal belief exemption allowing only children with serious health problems to opt out. – *Washington Post* (See item **13**)

- Security researchers from Trend Micro discovered a security flaw in the Android operating system's debugging component in which an attacker could create a special Executable and Linkable Format file to crash the debugger and view dumps and log files stored in memory, or to create a denial-of-service condition. – *Softpedia* (See item **21**)

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 26, Huntsville Times* – (Alabama**) Alabama Power agrees to shutter three coal-fired units, convert four others to natural gas in EPA deal**. The U.S. Department of Justice and the Environmental Protection Agency announced June 26 a settlement with Alabama Power to retire 3 coal-fired plants, convert 4 coal-fired plants to natural gas, pay a $100,000 fine, and spend at least $1.5 million to install electric charging infrastructure for airport service vehicles and company-owned cars.
Source:
http://www.al.com/news/index.ssf/2015/06/epa_alabama_power_agree_to_set.html

2. *June 25, WUSA 9 Washington, D.C.* – (Maryland**) 2500 gallons of fuel spill when truck overturns in Poolesville**. An overturned fuel truck spilled 2500 gallons of diesel fuel and prompted a HAZMAT response June 25 in Poolesville, Maryland.
Source: http://www.wusa9.com/story/news/local/2015/06/25/driver-hurt-in-poolesville-truck-accident/29259675/

3. *June 25, Vallejo Times Herald* – (California**) Valero refinery in Benicia to pay for air quality violations**. The Valero Refining Company will pay $122,500 in civil penalties to the Bay Area Air Quality Management District June 25 for numerous air quality violations at its Benicia, California refinery.
Source: http://www.timesheraldonline.com/general-news/20150625/valero-refinery-in-benicia-to-pay-for-air-quality-violations

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

4. *June 25, Detroit News* – (National**) Mitsubishi, Subaru recalling 600,000 U.S. vehicles.** Mitsubishi Motors North America issued recalls for 459,000 model year 2000 – 2005 vehicles of various models due to an issue with the passenger side sun visor that could cause it to detach if the passenger airbag deploys, as well as 74,000 model year 2006 – 2009 Eclipse and 2007 – 2009 Eclipse Spyder vehicles due to issues posed by rust inside the vehicle's anti-lock brake system. Subaru of America issued a separate recall June 25 for 74,000 model year 2015 Legacy, Impreza, XV Crosstrek, and 2016

WRX vehicles due to issues with the automatic pre-collision braking system.
Source:
http://www.detroitnews.com/story/business/autos/foreign/2015/06/25/mitsubishi-recall/29261775/

5. *June 25, Canton Repository* – (Ohio) **Fire damages United Surface Finishing plant in northeast Canton.** Authorities were investigating the cause of a June 25 fire at the United Surface Finishing plant in Canton, Ohio that prompted the plant's evacuation and a HAZMAT response. The plant sustained structural damage, and the roof was compromised in the vicinity of the blaze.
Source: http://www.cantonrep.com/article/20150625/NEWS/150629674

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

6. *June 25, Cleveland Plain Dealer* – (Ohio) **Three accused of Akron-based Ponzi scheme that cost investors $17 million.** Three Northeast Ohio men were indicted June 25 on charges alleging that they defrauded 70 investors out of $17 million from 2010 – 2014 by convincing them to give money to KGTA Petroleum Ltd., a company partially owned by one of the suspects, and spent the proceeds on luxury items and mortgage payments.
Source: http://www.cleveland.com/court-justice/index.ssf/2015/06/three_accused_of_akron-based_p.html

7. *June 25, Associated Press* – (Maryland) **Md. man charged with stealing from ATMs with skimming device.** A Riverdale, Maryland man was arrested June 24 on charges that he allegedly stole $300,000 from ATMs using skimming devices at a Sandy Spring Bank in Maryland.
Source: http://baltimore.cbslocal.com/2015/06/25/md-man-charged-with-stealing-from-atms-with-skimming-device/

8. *June 25, Boise Weekly* – (Idaho) **Hundreds of fraudulent credit cards seized, two suspects behind bars.** The Boise Police Department's Organized Retail Crime Unit arrested 2 suspects June 24 and seized 424 counterfeit credit and gift cards along with merchandise that they had bought with the fraudulent cards.
Source: http://www.boiseweekly.com/boise/hundreds-of-fraudulent-credit-cards-seized-two-suspects-behind-bars/Content?oid=3515991

[Return to top]

Transportation Systems Sector

9. *June 26, Associated Press* – (Tennessee) **I-75 reopens after 6 killed in wreck outside Chattanooga.** Interstate 75 in Chattanooga reopened June 26 after being closed for about 12 hours while crews cleared the scene of a 9-vehicle accident that killed 6 people June 25. The cause of the crash remains under investigation.
Source: http://www.msn.com/en-us/news/us/i-75-reopens-after-6-killed-in-wreck-outside-chattanooga/ar-AAc9l1w

10. *June 26, Longview Daily News* – (Washington) **One dead in crash that closed northbound I-5 near Chehalis.** Interstate 5 near mile post 71 in Chehalis was closed June 25 for 3 hours after a man was struck and killed by another car while assisting a broken down vehicle.
Source: http://tdn.com/news/local/one-dead-in-crash-that-closes-northbound-i--near/article_0051daf8-619e-5296-81cc-b40fb1bca710.html

Food and Agriculture Sector

Nothing to report

Water and Wastewater Systems Sector

11. *June 25, WDRB 41 Louisville* – (Kentucky) **Carrollton Utilities issues boil water advisory following 8-inch main break.** The Carrollton Utilities system in Louisville, Kentucky is under a boil water advisory June 25 after the water pressure fell when an 8-inch water main broke June 24. Crews are working to repair the water main.
Source: http://www.wdrb.com/story/29411517/carrollton-utilities-issues-boil-water-advisory-following-8-inch-main-break

12. *June 25, Atlantic Journal-Constitution* – (Georgia) **40,000 gallons of raw sewage leak into Lawrenceville lake.** About 40,000 gallons of raw sewage leaked from an 8-inch pipe close to Rhodes Jordan Park, in Lawrenceville, into a stream that empties into the park's lake. The leak will be continually monitored.
Source: http://www.ajc.com/news/news/local/40000-gallons-of-raw-sewage-leak-into-lawrencevill/nmmGZ/

Healthcare and Public Health Sector

13. *June 26, Washington Post* – (California) **The California Assembly just approved one of nation's strictest mandatory vaccine laws.** The California Assembly passed a bill

June 25 restricting exemptions for mandatory vaccination schedules, negating the State's personal belief exemption allowing only children with serious health problems to opt out.
Source: http://www.washingtonpost.com/news/morning-mix/wp/2015/06/26/the-california-assembly-just-approved-one-of-nations-strictest-mandatory-vaccine-laws/

14. *June 25, KXAS 5 Fort Worth* – (Texas) **Fake dentist accused of pulling 5 teeth from woman held on her couch: Dallas police.** A Honduran man and an accomplice are facing felony charges after allegedly impersonating a dentist and dental assistant and treating as many as 50 people without a medical license.
Source: http://www.nbcdfw.com/news/local/Man-Jailed-After-Pulling-Teeth-Claiming-to-be-a-Dentist-309824621.html

15. *June 25, Securityweek* – (National) **U.S. healthcare companies hardest hit by 'Stegoloader' malware.** Security researchers from Trend Micro reported that North American healthcare organizations are the primary victims of the Stegoloader Trojan, a malware identified as TROJ_GATAK which embeds malicious code in image files to avoid detection and has anti-virtual machine and anti-emulation capabilities to prevent analysis.
Source: http://www.securityweek.com/us-healthcare-companies-hardest-hit-stegoloader-malware

[Return to top]

Government Facilities Sector

16. *June 25, SC Magazine* – (Indiana) **Indiana town judge says attackers gained access to classified court records.** The FBI and Indiana Supreme Court announced June 25 they are investigating a June 23 breach of classified records at the Clarksville Town Court. Approximately 200 town employees are being notified of the data breach and are being given information on identity theft protection.
Source: http://www.scmagazine.com/indiana-town-judge-says-attackers-gained-access-to-classified-court-records/article/422932/

For another story, see item **18**

[Return to top]

Emergency Services Sector

17. *June 26, Associated Press* – (California) **2 San Diego firefighters stabbed by bystander at aid scene.** Two San Diego firefighters were hospitalized June 24 with multiple stab wounds after a bystander attacked them while they were responding to a 9-1-1 incident.
Source : http://abcnews.go.com/US/wireStory/san-diego-firefighters-stabbed-bystander-aid-scene-32029905

18. *June 25, WEAU 13 Eau Claire* – (Wisconsin**) Officers and jail inmates evacuated after person brings live explosive to law enforcement center**. Several law enforcement officers and prison inmates evacuated from the Ladysmith, Wisconsin Law Enforcement Center June 25, after a person brought a live World War II explosive to the police department. The inmates were brought to a Senior Center while the courthouse, police, and sheriff's offices were closed for the rest of the day.
Source : http://www.weau.com/home/headlines/Officers-and-jail-inmates-evacuated-after-person-brings-live-explosive-to-Law-Enforcement-Center-309910481.html

Information Technology Sector

19. *June 26, Softpedia* – (International) **Click-fraud attack morphs into ransomware risk in a couple of hours.** Security researchers at Damballa discovered that a threat actor dubbed RuthlessTreeMafia is distributing exploit kits along with the Rerdom malware in a click-fraud campaign in which they sell other threat actors access to infected users' systems. Researchers observed an infection result in the delivery of the CryptoWall ransomware.
Source: http://news.softpedia.com/news/click-fraud-attack-morphs-into-ransomware-risk-in-a-couple-of-hours-485395.shtml

20. *June 26, Securityweek* – (International) **Default SSH keys expose Cisco's virtual security appliances.** Cisco reported that customers using its Web Security, Email Security, and Security Management Virtual Appliances were vulnerable due to the products' use of default secure shell (SSH) keys, which could allow an unauthenticated, remote attacker to connect to a system with root user privileges. The company released a patch addressing the issue.
Source: http://www.securityweek.com/default-ssh-keys-expose-ciscos-virtual-security-appliances

21. *June 26, Softpedia* – (International) **94% of Android devices vulnerable to bug exposing memory content.** Security researchers from Trend Micro discovered security flaw in the Android operating system's (OS) debugging component in which an attacker could create a special Executable and Linkable Format (ELF) file to crash the debugger and view dumps and log files stored in memory, or to create a denial-of-service (DoS) condition. The issue affects all Android versions after 4.0, Ice Cream Sandwich.
Source: http://news.softpedia.com/news/94-of-android-devices-vulnerable-to-bug-exposing-memory-content-485382.shtml

22. *June 25, Threatpost* – (International) **Stored XSS flaw patched in Thycotic secret server.** Thycotic patched a stored cross-site scripting (XSS) vulnerability in its Secret Server product in which an attacker could use JavaScript code in the browser of a valid user to toggle the password mask and steal a victim's stored passwords.
Source: https://threatpost.com/stored-xss-flaw-patched-in-thycotic-secret-

server/113473

For another story, see item **15**

[[Return to top]]

Communications Sector

23. *June 25, Victorville Daily Press* – (California) **Verizon offering reward for copper theft information.** Verizon officials announced June 25 that the company is offering a reward of up to $10,000 for information leading to the arrest and prosecution of the suspect, or suspects, responsible for the theft of roughly 16,000 feet of copper communication cables throughout Southern California. The company has implemented "additional security measures" to prevent future thefts and is working with State and local law enforcement authorities.
Source: http://www.vvdailypress.com/article/20150625/NEWS/150629826

24. *June 25, Columbia Daily Herald* – (Tennessee) **Internet outages reported in area.** About 1,000 customers of Columbia Power and Water Systems (CPWS) and other Internet providers in Columbia, Tennessee experienced outages June 24 – June 25 after a laser in CPWS' data center was damaged and due to a fiber optic cable cut.
Source: http://columbiadailyherald.com/news/local-news/internet-outages-reported-area

25. *June 25, WBTA 1490 AM Batavia* – (New York) **WBTA to be temporarily off-air Friday morning.** WBTA Radio temporarily suspended AM and FM transmission June 26 in order to repair antenna damage caused by severe thunderstorms. While the stations are off-air, programming will continue on-line and via mobile devices.
Source: http://www.wbta1490.com/LocalNews/tabid/115/articleType/ArticleView/articleId/6322/WBTA-to-be-Temporarily-Off-Air-Friday-Morning.aspx

[[Return to top]]

Commercial Facilities Sector

26. *June 26, WFTS 28 Tampa* – (Florida) **Fire alarm wakes dozens at Empress Motel Efficiencies.** A June 26 fire at Empress Motel Efficiencies in St. Petersburg, Florida prompted 50 units to evacuate after 2 discarded mattresses outside a unit caught fire. Fire crews contained the incident and no injuries were reported.

Source: http://www.abcactionnews.com/news/region-south-pinellas/st-petersburg/fire-alarm-wakes-dozens-at-empress-motel-efficiencies

[Return to top]

<u>**Dams Sector**</u>

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.