Homeland Security

Daily Open Source Infrastructure Report 02 September 2016

Top Stories

- Two men were arrested in Torrance, California, August 30 for their roles in an $85,000 ATM skimming scheme. – *Southern California City News Service* (See item **2**)
- About 209 patients were evacuated from the Regional Medical Center Bayonet Point in Hudson, Florida, August 31 following an electrical fire in a generator room that knocked out power to the hospital. – *WFLA 8 Tampa* (See item **10**)
- More than 1,500 fire fighters reached 8 percent containment August 31 of the 17,302-acre Gap Fire burning in the Klamath National Forest between Yreka, California, and Happy Camp in Siskiyou County. – *Redding Record Searchlight* (See item **11**)
- Kimpton Hotel & Restaurant Group, LLC officials confirmed August 31 that credit and debit cards used at more than 60 restaurants and hotel reception desks from February 2016 – July 2016 may have been compromised by malware. – *Krebs on Security* (See item **17**)

Fast Jump Menu

Energy Sector

Nothing to report

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

1. *August 31, KTLA 5 Los Angeles* – (California) **FBI seeks help identifying 'Helmet Head Bandit' in connection with 2 recent bank robberies.** Authorities are searching August 31 for a man dubbed the "Helmet Head Bandit" who is suspected of robbing 2 banks in La Canada Flintridge and Tujunga, California, and attempting to rob 1 other in Tujunga August 31.
   Source: http://ktla.com/2016/08/31/fbi-seek-help-identifying-helmet-head-bandit-in-connection-with-3-recent-bank-robberies

2. *August 31, Southern California City News Service* – (California) **Duo arrested in widespread LA ATM machine skimming scam.** Two men were arrested in Torrance, California, August 30 for their roles in an $85,000 ATM skimming scheme where the duo installed skimming devices on ATM machines in Burbank and elsewhere in Los Angeles County and stole the account information from over 50 bank customers to create cloned ATM cards and withdraw cash from other ATMs in the county. Officials discovered an additional $233,000 in declined transactions attempted by the duo.
   Source: http://patch.com/california/northhollywood/duo-arrested-widespread-la-atm-machine-skimming-scam

Transportation Systems Sector

3. *September 1, Philadelphia Inquirer* – (Pennsylvania) **I-95 reopens after fire truck, tractor trailer crash.** A 2-vehicle crash involving a semi-truck and a fire truck forced the closure of southbound Interstate 95 in Philadelphia, Pennsylvania, for several hours August 31 and sent 5 firefighters to an area hospital with injuries.
   Source: http://www.philly.com/philly/blogs/in-transit/Big-delays-on-Interstate-95-

South-after-fire-truck-tractor-trailer-crash.html

4. *September 1, WSCH 99.3 FM Aurora* – (Ohio) **Accident cripples traffic on I-275/74 in Ohio.** Interstate 275 and Interstate 74 near Ronald Reagan Highway in Hamilton County, Ohio, were closed for over 3 hours September 1 while crews worked to clear the wreckage from two unrelated crashes.
Source: http://eaglecountryonline.com/local-article/accident-cripples-traffic-on-i-27574-in-ohio/

5. *September 1, KTBS 3 Shreveport* – (Louisiana) **I-20E reopened following fatal crash near Dixie Inn.** Eastbound lanes of Interstate 20 near Dixie Inn, Louisiana, were closed for several hours August 31 while crews worked to clear the wreckage from a crash involving 2 semi-trucks and 5 other vehicles that killed 1 person and injured another. Traffic was diverted to Highway 80 at the Goodwill Road exit while officials investigated the scene.
Source: http://www.ktbs.com/story/32943351/major-crash-reported-on-interstate-20-near-dixie-inn

6. *August 31, KNTV 11 San Jose; San Francisco Bay City News* – (California) **Mother of young girls killed in Petaluma River crash was driving without license: CHP.** Northbound Petaluma Boulevard between Gossage Avenue and Skillman Lane in Petaluma, California, was closed for nearly 6 hours August 31 while officials investigated the scene of a single-vehicle crash after a car slid off the road and overturned in the Petaluma River. Two people were killed and another was injured.
Source: http://www.nbcbayarea.com/news/local/Two-Children-Involved-in-Major-Injury-Accident-in-Petaluma-391895651.html

7. *August 31, KTVI 2 St. Louis* – (Missouri) **Fatal accident on Highway 21 in De Soto MO.** A 2-vehicle crash forced the closure of Highway 21 in DeSoto, Missouri, for more than 3 hours August 31 while Missouri Highway Patrol investigated the scene of the crash and crews cleared the wreckage. One person was killed.
Source: http://fox2now.com/2016/08/31/fatal-accident-on-highway-21-in-de-soto-mo/

Food and Agriculture Sector

8. *August 31, Visalia Times-Delta* – (California) **Ruiz Foods closes after insects were found at the facility.** Ruiz Foods officials reported August 31 that the Ruiz Foods facility in Dinuba, California, was closed until further notice after Federal personnel discovered insects in the food processing facility. A company spokesperson stated no food-borne or product contamination issues were found at the plant.
Source: http://www.visaliatimesdelta.com/story/news/local/2016/08/31/ruiz-foods-closes-insects-found-facility/89684200/

9. *August 31, U.S. Food and Drug Administration* – (National) **Voluntary recall of cartons of Entenmann’s Little Bites Fudge Brownies 5 pack (best by date Oct 8, 2016), Chocolate Chip Muffins 5 pack and 10 pack (best by date Oct 8, 2016) and Variety 20 Pack – Fudge Brownies, Chocolate Chip Muffins and Blueberry**

Muffins (best by date Sep 24, 2016) due to choking and/or cutting hazard from presence of small pieces of plastic. Bimbo Bakeries USA, Inc., issued a voluntary recall August 31 for its Entenmann's Little Bites Fudge Brownies, Entenmann's Little Bites Chocolate Chip Muffins, and Entenmann's Little Bites Variety Pack products after the company received a consumer report stating plastic fragments were found in the products following a manufacturing failure at a third-party bakery. One adverse reaction has been reported and the products were distributed to retail stores nationwide.
Source: http://www.fda.gov/Safety/Recalls/ucm518835.htm

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

10. *September 1, WFLA 8 Tampa* – (Florida) **Electrical fire forces Florida hospital to evacuate as Tropical Storm Hermine nears.** A total of 209 patients were evacuated from the Regional Medical Center Bayonet Point in Hudson, Florida, August 31 following an electrical fire in a generator room that knocked out power to the hospital. Officials stated nearly 50 patients were transferred to Oak Hill Hospital in Brooksville and the other patients were transported to regional facilities.
Source: http://wsav.com/2016/09/01/electrical-fire-forces-florida-hospital-to-evacuate-as-tropical-storm-hermine-nears/

Government Facilities Sector

11. *September 1, Redding Record Searchlight* – (California) **Gap Fire in Siskiyou County grows to over 17,000 acres.** More than 1,500 fire fighters reached 8 percent containment August 31 of the 17,302-acre Gap Fire burning in the Klamath National Forest between Yreka, California, and Happy Camp in Siskiyou County, which has destroyed at least 9 structures and 12 outbuildings.
Source: http://www.redding.com/news/local/gap-fire-in-siskiyou-county-grows-to-over-13000-acres-3b667660-1063-3abb-e053-0100007fbdfd-391970221.html

12. *September 1, Riverside Press-Enterprise* – (California) **Firefighters gain 60 percent containment on 1,470-acre Bogart fire as fire activity dies down.** Crews reached 60 percent containment August 31 of the 1,470-acre Bogart Fire burning in the Cherry Valley area of California.
Source: http://www.pe.com/articles/fire-812042-bogart-named.html

Emergency Services Sector

Nothing to report

Information Technology Sector

13. *September 1, SecurityWeek* – (International) **Betabot starts delivering Cerber**

ransomware. Security researchers from Invincea discovered the Betabot ransomware began carrying out a second-stage payload where the malware delivers the Cerber ransomware on the endpoint of a compromised machine after stealing user passwords in the first-stage, in order for the malware operators to increase their profits. Researchers also found the ransomware was being delivered by the Neutrino exploit kit (EK) and stated the malware avoids detection and analysis through virtual machine awareness and by checking for sandboxes.
Source: http://www.securityweek.com/betabot-starts-delivering-cerber-ransomware

14. *September 1, SecurityWeek* – (International) **Cisco fixes severe flaw in WebEx, small business products.** Cisco released software and firmware updates addressing several vulnerabilities in its WebEx Meetings Player version T29.10 for WebEx Recording Format (WRF) files after a COSIG security researcher discovered a critical flaw that could allow an unauthenticated attacker to execute arbitrary code remotely by tricking a user to open a specially crafted file, and a medium severity vulnerability that could allow an unauthenticated attacker to remotely crash the program by convincing the user to access a malicious file. Cisco also released fixes for three denial-of-service (DoS), cross-site request forgery (CSRF), and cross-site scripting (XSS) issues plaguing its Small Business 220 Series Smart Plus (Sx220) switches that could allow a remote, unauthenticated attacker to gain access to Simple Network Management Protocol (SNMP) objects on a compromised device.
Source: http://www.securityweek.com/cisco-fixes-severe-flaws-webex-small-business-products

15. *September 1, Softpedia* – (International) **Vulnerability in Yandex browser allows attackers to steal victims' browsing data.** A security researcher from Netsparker discovered the login form of the Yandex Browser was plagued with a cross-site forgery request (CSRF) vulnerability that could allow an attacker to steal a victim's passwords, bookmarks, autocomplete info, and browser history, among other data, by convincing a user to visit a malicious Website that includes code to create a Yandex Browser data sync login form and submits the information with the attacker's credentials, thereby starting an automatic syncing process that sends a copy of the user's data to the attacker.
Source: http://news.softpedia.com/news/vulnerability-in-yandex-browser-allows-attackers-to-steal-victim-s-browsing-data-507848.shtml

16. *August 31, SecurityWeek* – (International) **Adobe patches critical vulnerability in ColdFusion.** Adobe released security updates for ColdFusion versions 10 and 11 resolving a critical vulnerability after a researcher from legalhackers.com discovered the flaw is related to parsing specially crafted XML entities and could lead to information disclosure. Adobe officials advised users to install the patches and apply secure configuration settings to avoid the security flaw.
Source: http://www.securityweek.com/adobe-patches-critical-vulnerability-coldfusion

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

Nothing to report

Commercial Facilities Sector

17. *September 1, Krebs on Security* – (National) **Kimpton Hotels acknowledges data breach.** Officials from the Kimpton Hotel & Restaurant Group, LLC confirmed August 31 that malware detected on payment terminals may have compromised credit and debit cards used at more than 60 restaurants and hotel reception desks from February 16, 2016 – July 7, 2016. The source and extent of the breach remains under investigation.
    Source: http://krebsonsecurity.com/2016/09/kimpton-hotels-acknowledges-data-breach/

Dams Sector

Nothing to report

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

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.