Homeland Security

Daily Open Source Infrastructure Report 12 July 2016

Top Stories

- Security researchers from IBM’s X-Force Research reported that the GootKit trojan, which targets banks internationally, has updated its source and mode of operation to avoid antivirus detection by changing its installation method. – *Softpedia* (See item **4**)

- The FBI offered a reward July 8 in exchange for information leading to the capture of a man dubbed the “Hipster Bandit” who is suspected of robbing eight banks and attempting to rob two others in San Diego County since September 2015. – *KNSD 39 San Diego* (See item **5**)

- Officials announced July 11 that 2 Alabama campers were arrested for arson in the Cold Springs Fire which grew to 538 acres and forced the evacuation of nearly 2,000 residents near Boulder County, Colorado. – *KUSA 9 Denver* (See item **22**)

- Omni Hotels & Resorts reported July 8 that its point-of-sale (PoS) systems were allegedly compromised after discovering malware attacks on its network May 30, which intended to collect payment card data. – *IDG News Service* (See item **25**)

Fast Jump Menu

Energy Sector

1. *July 11, Detroit News* – (Michigan) **After storms, 150 homes still without power.** DTE Energy crews worked July 11 to restore power to about 150 customers who remained without service following a series of storms that moved through southeast Michigan July 7 – July 8 and knocked out electricity to nearly 120,000 customers.
   Source: http://www.detroitnews.com/story/news/local/wayne-county/2016/07/08/storms-knock-power/86886302/

Chemical Industry Sector

2. *July 10, WTAE 4 Pittsburgh* – (Pennsylvania) **More than fourteen stations called to Washington County chemical fire.** The National Polymers Inc., in Washington County sustained severe damage July 9 due to an alleged accidental fire that prompted fire crews to remain on site for over two hours. The building was ventilated and the incident was contained before the fire reached stored chemicals.
   Source: http://www.wtae.com/news/more-than-fourteen-stations-called-to-washington-county-chemical-fire/40434688

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

3. *July 8, Associated Press* – (International) **California man arrested on spy charges involving satellites.** A California man was arrested and charged July 7 with allegedly attempting to sell sensitive information used in military and commercial satellites to an individual whom he believed was a foreign agent.
   Source: http://www.foxnews.com/us/2016/07/08/california-man-arrested-on-spy-charges-involving-satellites.html

Financial Services Sector

4. *July 11, Softpedia* – (International) **GootKit banking trojan receives massive update.** Security researchers from IBM's X-Force Research reported that the GootKit trojan, which targets banks internationally, has updated its source and mode of operation to avoid antivirus detection by changing its installation method to use scheduled tasks that run every minute, allowing the trojan to run with least-privilege user accounts (LUA) and administrator accounts.
   Source: http://news.softpedia.com/news/gootkit-banking-trojan-receives-massive-update-506181.shtml

5. *July 8, KNSD 39 San Diego* – (California) **FBI seeks ‘Hipster Bandit,’ offers $20K reward.** The FBI offered a reward July 8 in exchange for information leading to the capture of a man dubbed the “Hipster Bandit” who is suspected of robbing eight banks and attempting to rob two others in San Diego County since September 2015, including a Wells Fargo Bank branch July 2.
   Source: http://www.nbcsandiego.com/news/local/San-Diego-County-Hipster-Bandit-Sought-by-FBI-20K-Reward-386076441.html

6. *July 7, U.S. Attorney’s Office, District of Connecticut* – (Connecticut) **Norwich resident admits role in insurance fraud scheme.** A Norwich, Connecticut resident pleaded guilty July 7 for his role in an insurance fraud scheme where he and co-conspirators staged approximately 50 car crashes in southeastern Connecticut, and filed fraudulent property damage and bodily injury claims with various automobile insurance companies in order to collect up to $30,000 in insurance payouts per fraudulent claim between April 2011 and February 2014.
   Source: https://www.justice.gov/usao-ct/pr/norwich-resident-admits-role-insurance-fraud-scheme

Transportation Systems Sector

7. *July 11, KHOU 11 Houston* – (Texas) **United flight aborts takeoff, blows tires at Bush Airport.** United Flight 1594 was forced to abort its take off from Bush Intercontinental Airport in Houston July 11 due to a possible mechanical issue that caused two tires to blow out.
   Source: http://www.khou.com/news/local/emergency-response-on-united-flight-leaving-bush-airport/269587425

8. *July 10, KEYE 42 Austin* – (Texas) **Highway 71 reopened after fatal crash.** State Highway 71 was closed for approximately 3 hours after a multi-vehicle crash left one person dead July 10 in Llano County.
   Source: http://keyetv.com/news/local/one-person-dead-in-llano-after-highway-crash

9. *July 9, KNBC 4 Los Angeles* – (California) **Baby, toddler among 3 killed in crash on 91 Freeway near Cerritos.** A three-vehicle crash on 91 Freeway near Cerritos closed four lanes for about 4 hours July 9 after a vehicle hit a gas tanker and overturned. The incident led to three deaths and two minor injuries
   Source: http://www.nbclosangeles.com/news/local/Lanes-Closed-3-Killed-Crash-91-Freeway-in-Cerritos-386130201.html

10. *July 9, Seattle Times* – (Washington) **Semi-truck driver, 65, killed in crash near Bothell.** Northbound and southbound lanes of Highway 522 were closed for nearly 8 hours July 8 while crews worked to clear the wreckage from a six-vehicle crash involving a semi-truck that killed one person. The cause of the accident is under investigation.
    Source: http://www.seattletimes.com/seattle-news/transportation/interstate-405-closed-in-bothell-area-after-fatal-semi-truck-crash/

11. *July 9, KOLO 8 Reno* – (Nevada) **Both lanes of Pyramid Highway open in Spanish Springs after fatal accident.** A rollover crash on Pyramid Highway in Sparks, Nevada closed the highway for several hours, left one woman dead, and sent four others to the hospital with injuries July 9.
Source: http://www.kolotv.com/content/news/Both-directions-of-Pyramid-Highway-closed-in-Spanish-Springs-for-accident-386144271.html

12. *July 9, Associated Press –* (Connecticut) **American Airlines flight makes emergency landing at Bradley.** American Airlines Flight 1692 from Charlotte, North Carolina was forced to make an emergency landing at Bradley International Airport in Windsor Locks July 9 due to mechanical issues. Officials declared a state of emergency to allow the plane to land quickly.
Source: http://fox61.com/2016/07/09/plane-makes-emergency-landing-at-bradley/

Food and Agriculture Sector

13. *July 11, U.S. Food and Drug Administration* – (National) **Continental Mills recalls Blueberry Pancake Mix because of possible health risk.** Continental Mills, Inc., issued a nationwide recall July 9 for its Krusteaz Blueberry Pancake Mix products sold in two variations due to potential E.coli O121 contamination after the company's supplier notified the firm that the blueberry nugget ingredient used in the pancake mix contains flour, which was recalled by General Mills, Inc., due to potential E. coli O121 contamination. Officials urged consumers diagnosed with E.coli O121 to contact State and local public health officials.
Source: http://www.fda.gov/Safety/Recalls/ucm510486.htm

14. *July 10, U.S. Department of Agriculture* – (National) **Kabob's Acquisition, Inc. recalls not ready-to-eat meat and poultry products due to possible E.coli O121 contamination.** Kabob's Acquisition, Inc., issued a recall July 8 for approximately 44,850 pounds of its raw intact and heat treated, not ready-to-eat meat and poultry products sold in 28 variations due to potential E.coli O121 contamination after the company's supplier notified the firm that General Mills, Inc., recalled the flour used in the meat products due to possible association with a multi-state E.coli O121 outbreak. There have been no confirmed reports of adverse reactions and the products were distributed to hotel, restaurant, and institutional locations nationwide.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-057-2016-release

15. *July 9, U.S. Food and Drug Administration* – (National) **Kroger recalls Deluxe S'mores Ice Cream due to undeclared allergens.** The Kroger Co., issued a recall July 9 for its Kroger Deluxe S'mores Ice Cream products sold in 48-ounce packages due to undeclared peanuts after the company's supplier, Grain Craft, notified the firm that a raw ingredient used in the ice cream products may have been contaminated with low levels of peanut residue. No illnesses have been reported and the products were sold at stores operating under 14 names in 29 States.
Source: http://www.fda.gov/Safety/Recalls/ucm510483.htm

16. *July 8, U.S. Food and Drug Administration* – (Washington) **Hearn Kirkwood recalls "Evie's Cheddar Potato Salad" because of possible health risk.** Hearn Kirkwood issued a voluntary recall July 6 for its Evie's Cheddar Potato Macaroni Salad products sold in 6-ounce packages due to potential Listeria monocytogenes contamination after the company's frozen green peas supplier, National Frozen Foods Corporation, recalled the peas used in the products due to Listeria. No illnesses have been reported and the products were sold to Amazon Fresh locations in Bellevue, Washington.
Source: http://www.fda.gov/Safety/Recalls/ucm510429.htm

For another story, see item **28**

Water and Wastewater Systems Sector

17. *July 10, WOWT 6 Omaha* – (Nebraska) **Fremont awaiting final test result on drinking water safety.** A lightning strike July 7 at a water treatment plant prompted officials to issue a boil water advisory for residents of Fremont, Nebraska until final water testing confirmed safe drinking water.
Source: http://www.wowt.com/content/news/Fremont-awaiting-final-test-result-on-drinking-water-safety-386160471.html

18. *July 8, Hawaii News Now* – (Hawaii) **9,000 gallons of sewage spill into water at Hickam Beach.** Official posted warning signs at Hickam Beach in Honolulu July 8 after a water main break in Joint Base Pearl-Harbor Hickam ruptured, spilling 9,000 gallons of sewage into the Hickam Beach. The Department of Health was testing the water.
Source: http://www.hawaiinewsnow.com/story/32404669/9000-gallons-of-sewage-spill-into-water-at-hickam-beach

Healthcare and Public Health Sector

19. *July 11, Torrington Register Citizen; Connecticut Health I-Team* – (National) **Connecticut hospitals facing acute drug shortages must do workarounds.** The U.S. Food and Drug Administration updated its list of acute-drugs that are in short supply nationally, which include antibiotics, intravenous saline, and morphine, among others July 11. The shortages have forced hospitals across Connecticut to turn to alternative drugs, ration supplies, or seek new suppliers to work around the shortages.
Source: http://www.registercitizen.com/article/RC/20160711/NEWS/160719955

20. *July 8, WSVN 7 Miami* – (Florida) **All clear given after phone threats lead to evacuation of Nicklaus Children's Hospital.** Employees at Nicklaus Children's Hospital in south Miami-Dade County were evacuated while patients were locked in their rooms for approximately 5 hours July 8 due to a phoned-in bomb threat and possible active shooter. Police issued an all-clear and the hospital resumed operations after nothing suspicious was found.
Source: http://wsvn.com/news/local/police-situation-at-nicklaus-childrens-hospital/

Government Facilities Sector

21. *July 11, KMGH 7 Denver* – (Colorado) **Hayden Pass Fire in Coaldale grows to 5,000 acres; pre-evacuation notices sent to nearby homes.** Crews worked July 11 to contain the 5,000-acre Hayden Pass Fire burning near Hayden Creek in Colorado after authorities issued an Air Quality Advisory and pre-evacuation notice for homes along County Road 6 to Pole Mountain lane.
Source: http://www.thedenverchannel.com/news/wildfire/hayden-pass-fire-grows-to-5000-acres

22. *July 11, KUSA 9 Denver* – (Colorado) **2 campers arrested for arson in Cold Springs Fire.** The Boulder County Sheriff's Office announced July 11 that 2 Alabama campers were arrested for arson in the Cold Springs Fire which grew to 538 acres and forced the evacuation of nearly 2,000 residents near Boulder County, Colorado.
Source: http://www.9news.com/news/local/wildfires/2-campers-arrested-for-arson-in-cold-springs-fire/268906229

23. *July 10, San Gabriel Valley Tribune; Los Angeles Daily News* – (California) **Sage Fire: 750 homes evacuated, more than 800 acres burned near Santa Clarita.** Crews reached 15 percent containment July 9 of the 800-acre Sage Fire burning west of Santa Clarita. About 200 firefighters are working to contain the blaze and evacuation orders were issued for approximately 2,000 residents.
Source: http://www.dailynews.com/general-news/20160709/sage-fire-750-homes-evacuated-more-than-800-acres-burned-near-santa-clarita

Emergency Services Sector

Nothing to report

Information Technology Sector

24. *July 11, Softpedia* – (International) **MIUI vulnerability affects millions of Xiaomi Android devices.** Security researchers from IBM's Security Intelligence team reported that a remote code execution (RCE) vulnerability exists in MIUI analytics component in versions prior to MIUI Global Stable 7.2 after researchers discovered that the self-update mechanism can be hijacked via a Man-in-the-Middle (MitM) attack and used to deliver malicious update packages. The analytics package uses Hypertext Transfer Protocol (HTTP) to query an update server for upgrades and downloads the update requests, allow attackers to watch for requests and use basic spoofing techniques.
Source: http://news.softpedia.com/news/miui-vulnerability-affects-millions-of-xiaomi-android-devices-506185.shtml

For another story, see item **4**

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

25. *June 11, IDG News Service* – (National) **Omni Hotels was hit by point-of-sale malware.** Omni Hotels & Resorts reported July 8 that its point-of-sale (PoS) systems were allegedly compromised after discovering malware attacks on its network May 30, which were intended to collect certain payment card information including cardholder names, credit/debit card numbers, security codes, and expiration dates. The luxury hotel did not disclose how many of its 60 properties were affected.
Source: http://www.computerworld.com/article/3093390/security/omni-hotels-was-hit-by-point-of-sale-malware.html#tk.rss_security

26. *July 11, WBTW 13 Florence* – (North Carolina) **NC church to rebuild after fire from 2 lightning strikes destroys building.** The Cricket Ridge Pentecostal Freewill Baptist Church in Wayne County was destroyed July 7 after severe storms caused lightning to strike the church twice, causing the building to ignite in flames. The flames were extinguished and no injuries were reported.
Source: http://wbtw.com/2016/07/11/nc-church-to-rebuild-after-fire-from-2-lightning-strikes-destroys-building/

27. *July 10, WSAV 3 Savannah* – (Georgia) **Red Cross assists those displaced in Georgetown apartment fire.** Twenty-four apartment units were damaged and at least 50 residents were displaced from the Preston Grove Apartments in Savannah, Georgia July 10 due to a fire that allegedly began from a discarded cigarette left on a porch. A few residents were injured and the incident was contained.
Source: http://wsav.com/2016/07/10/emergency-crews-on-scene-of-georgetown-apartment/

Dams Sector

28. *July 8, Kalamazoo Gazette* – (Michigan) **Dam repair robs crops of water during critical time, farmers say.** Officials reported July 8 that emergency repairs on the Sturgis Dam in Michigan caused river levels upstream to fall below normal levels and caused farmers to incur a deficiency in water as the intake pipes could not draw water from the low river. Officials alerted the public July 2 that the city of Sturgis would

begin a drawdown of the reservoir area upstream to allow repair work of the dam. Source: http://www.mlive.com/news/kalamazoo/index.ssf/2016/07/dam_work_robs_crops_of_water_d.html

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.