Homeland Security

Daily Open Source Infrastructure Report
11 February 2016

Top Stories

- Daimler AG and Volkswagen issued precautionary recalls February 10 for a total of 1.5 million vehicles sold in the U.S. due to potentially faulty Takata Corporation airbags. – *CNN Money* (See item **3**)

- Officials issued a precautionary boil-water advisory for Flint, Michigan residents February 10 after a February 9 water main break. – *CNN* (See item **10**)

- Security researchers from Kaspersky Lab researchers reported that the Poseidon Group has been targeting international financial sectors, telecommunications sectors, critical manufacturing sectors, and energy sectors to collect information from company networks via spear-phishing packages. – *The Register* (See item **22**)

- Five men in Jacksonville, Florida, were arrested February 9 and charged for their involvement in a grand theft cargo scheme that netted $1.5 million. – *WJXT 4 Jacksonville* (See item **27**)

Fast Jump Menu

Energy Sector

1. *February 9, Casper Star-Tribune* – (Wyoming) **Wyoming passes new flaring rule amid praise and criticism.** The Wyoming Oil and Gas Conservation Commission approved new regulations February 9 aimed at curbing methane emissions from oil wells, which include requirements for operators to report what is being emitted and whether it is being vented or flared, as well as lowering the daily venting limit from 60,000 cubic feet of gas to 20,000 cubic feet, among other regulations.
Source: http://trib.com/business/energy/wyoming-passes-new-flaring-rule-amid-praise-and-criticism/article_2ac33e2d-83cb-577b-9945-9ac76ef60669.html

2. *February 9, Ames Tribune* – (Iowa) **Firefighters respond to smoke at power plant.** A February 9 fire at Ames Power Plant in Iowa shut down operations for more than 2 hours after smoke was detected from the refuse derived fuel (RDF) bin near the plant which stores RDF from the Resource Recover Plant. The fire was contained in the bin and the cause remains under investigation.
Source: http://amestrib.com/news/ames-and-story-county/firefighters-respond-smoke-power-plant

For another story, see item **22**

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

3. *February 10, CNN Money* – (National) **German carmakers recall U.S. vehicles over airbags.** Daimler AG and Volkswagen issued precautionary recalls February 10 for a total of 1.5 million vehicles sold in the U.S. due to potentially faulty Takata Corporation airbags that can explode when activated and release shrapnel inside the vehicle, which has resulted in 9 deaths in the U.S. The recall includes 840,000 model years 2005 – 2014 Daimler vehicles and 680,000 model years 2006 – 2014 Volkswagen vehicles.
Source: http://money.cnn.com/2016/02/10/news/companies/daimler-takata-airbag-recall/

For another story, see item **22**

Defense Industrial Base Sector

See item **22**

Financial Services Sector

4. *February 9, U.S. Securities and Exchange Commission* – (International) **Monsanto paying $80 million penalty for accounting violations.** The U.S. Securities and Exchange Commission (SEC) announced February 9 that St. Louis-based Monsanto Company agreed to pay an $80 million penalty and retain an independent compliance consultant to settle charges that the company violated accounting rules and misstated company earnings related to a rebate program tied its flagship product, Roundup, after an SEC investigation found that the company improperly accounted for millions of dollars in rebates to retailers and distributors and misstated its consolidated earnings during a 3-year period. Three accounting and sales executives also agreed to pay penalties for their roles in the scheme.
Source: https://www.sec.gov/news/pressrelease/2016-25.html

5. *February 9, U.S. Attorney's Office, Northern District of Alabama* – (National) **IRS employee pleads guilty to $1 million ID theft tax fraud scheme.** A former U.S. Internal Revenue Service (IRS) employee who worked in the Taxpayer Advocate Services office in Alabama pleaded guilty February 8 in Federal court for her role in a tax-fraud scheme where she used her IRS computer access to steal taxpayers' identities and file up to $1.5 million in fraudulent tax returns from 2008 – 2011. The former employee worked with three other co-conspirators who were charged for their roles in the scheme.
Source: http://www.justice.gov/usao-ndal/pr/irs-employee-pleads-guilty-1-million-id-theft-tax-fraud-scheme

For another story, see item **22**

Transportation Systems Sector

6. *February 10, WHKY 14 Hickory* – (North Carolina) **Tuesday afternoon accident closes Highway 127 in Hickory.** Highway 127 in Hickory was closed for over 4 hours February 9 after a vehicle ran off the road and hit a pole and another vehicle. No injuries were reported.
Source: http://www.whky.com/archive/item/9949-tuesday-afternoon-accident-closes-highway-127-in-hickory#.VrtvwbIrKUk

7. *February 9, Grand Forks Herald* – (North Dakota) **Highway patrol: 4 injured in I-29 pile up Monday that could've been avoided.** A 12-vehicle pileup on Interstate 29 in Bowesmont closed the highway for more than 11 hours and injured 4 people February 9 while officials investigated the scene of the crash and crews worked to remove the wreckage.
Source: http://www.grandforksherald.com/news/region/3944230-highway-patrol-4-injured-i-29-pile-monday-couldve-been-avoided

8. *February 9, KSTU 13 Salt Lake City* – (Utah) **Provo Canyon reopens after semi overturns, spills fertilizer on roadway.** Eastbound lanes of Highway 189 in Provo Canyon were shut down for more than 3 hours February 9 while crews worked to clear

the wreckage from an overturned semi-truck that spilled ammonium nitrate fertilizer.
Source: http://fox13now.com/2016/02/09/semi-crash-closes-provo-canyon-both-directions-may-not-open-for-hours/

For another story see item **14**

Food and Agriculture Sector

9. *February 9, U.S. Department of Agriculture* – (Texas; Louisiana) **Hormel Foods Corporation recalls beef products due to possible foreign matter contamination.** Hormel Foods Corporation issued a recall February 9 for approximately 450 pounds of its Dinty Moore Hearty Meals No Preservatives Beef Stew products sold in 15-ounce cans after a routine inspection revealed the presence of extraneous materials from the production area. The products were distributed to Kroger retail locations in Texas and Louisiana.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-015-2016-release

For another story, see item **4**

Water and Wastewater Systems Sector

10. *February 10, CNN* – (Michigan) **Adding insult to injury: Flint issues boil-water advisory after water main break.** Officials announced a precautionary boil-water advisory for Flint residents February 10 after a February 9 water main break decreased water pressure and may have allowed bacteria in the water. In addition, the governor of Michigan asked for an additional $195 million in funding for the current lead water crisis.
Source: http://www.cnn.com/2016/02/10/politics/flint-water-crisis/

11. *February 10, WRDW 12 Augusta* – (Georgia) **Schools closed, hospitals and restaurants impacted after boil water advisory.** A boil water advisory February 10 in Richmond County closed all county public school while officials tested turbidity limits from the Highland Avenue Water Treatment Plant. Officials reported that no evidence of contamination was confirmed.
Source: http://www.wrdw.com/home/headlines/Boil-Water-Notice-issued-for-part-of-Augusta-368236491.html

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

12. *February 10, Cleveland Plain Dealer* – (National) **Thieves use 464,000 stolen Social Security numbers to attack IRS' website.** The U.S. Internal Revenue Service announced February 9 that thieves used computer malware to attack its official Web

site and conduct 464,000 unauthorized attempts to generate e-file personal identification numbers (PINs) in order to file returns for stolen Social Security numbers, 101,000 of which were successful. Officials stated that the Social Security numbers used were stolen from other sources and that an investigation into the incident is ongoing.
Source: http://www.cleveland.com/business/index.ssf/2016/02/thieves_use_464000_stolen_soci.html

13. *February 10, Associated Press* – (Michigan) **Authorities: Icy roads likely factor in crash that killed 2.** Schools in Holland, Zeeland, and Grand Haven were among the several schools that closed February 10 in Michigan due to heavy snowfall and hazardous roads conditions.
Source: http://www.9and10news.com/story/31185425/many-schools-closed-for-day-after-snow-dumps-on-michigan

14. *February 9, KDVR 31 Denver* – (Colorado) **All clear given at State Capitol after threat forces evacuation.** The State Capitol building in Denver was evacuated for 3 hours February 9 due to a hoax bomb threat. Officials stated that normal operations would resume February 10.
Source: http://kdvr.com/2016/02/09/capitol-evacuated-after-bomb-threat-called-into-police/

For additional stories, see items **5**, **11**, and **23**

Emergency Services Sector

Nothing to report

Information Technology Sector

15. *February 10, Softpedia* – (International) **Linode VPS host accidentally deploys servers with the same SSH key.** Linode reported that its virtual private servers (VPS) hosted on Ubuntu machines could have been susceptible to man-in-the-middle (MitM) attacks after the company disseminated Ubuntu 15.0 images to some of its clients' server, which used the same hard-coded secure shell (SSH) key. The company stated its customers need to reconfigure the SSH daemon and run a specific shell command to fix the vulnerability.
Source: http://news.softpedia.com/news/linode-vps-host-accidentally-deploys-servers-with-the-same-ssh-key-500192.shtml

16. *February 10, SecurityWeek* – (International) **Microsoft patches critical flaws in Windows, Browsers.** Microsoft released several patches for its products including patches for 22 Flash Player flaws used in Internet Explorer 10, 11, and Edge, and patched a critical memory corruption flaw in Windows Journal, a remote code execution (RCE) flaw, and a denial-of-service (DoS) flaw, among other patched vulnerabilities.

Source: http://www.securityweek.com/microsoft-patches-critical-flaws-windows-browsers

17. *February 10, IDG News Service* – (International) **Google will stop accepting new Flash ads on June 30.** Google reported that it will stop accepting new Adobe Flash-based display ads for AdWords and DoubleClick Digital Marketing, and will not permit Flash ads on its Display Network or DoubleClick after January 2017 due to the frequent security vulnerabilities within Flash Players.
Source: http://www.computerworld.com/article/3031908/security/google-will-stop-accepting-new-flash-ads-on-june-30.html#tk.rss_security

18. *February 9, Softpedia* – (International) **Tool for hacking facebook accounts contains Remtasu spyware.** The Win32/Remtasu.Y malware, also known as Remtasu, was reported infecting computer systems through different variants and through an app named Hack Facebook to log keystrokes, steal data from clipboard, save the information to local files, and upload the information to a remote file transfer protocol (FTP) server by duplicating itself to the Windows System32 folder saved as InstallerDir and creating a registry key that executes the malware process each time a user starts their computer. Researchers reported an antivirus program should help detect the malware.
Source: http://news.softpedia.com/news/tool-for-hacking-facebook-accounts-contains-remtasu-spyware-500132.shtml

19. *February 9, SecurityWeek* – (International) **Nuclear EK gate uses decoy CloudFlare DDoS check page.** Security researchers from Malwarebytes reported that hackers were using malvertising attacks to deceive users into visiting a rogue domain similar to CloudFlare's distributed denial of service (DDoS) check page, that contained the Nuclear exploit kit (EK) to compromise a user's system. CloudFlare reported the fraudulent domain was not associated with its security firm.
Source: http://www.securityweek.com/nuclear-ek-gate-uses-decoy-cloudflare-ddos-check-page

20. *February 9, SecurityWeek* – (International) **Adobe patches flaws in Flash, Photoshop, Connect.** Adobe release security updates and patches for its Flash Player, Photoshop, Bridge, Connect, and Experience Manager that addressed several vulnerabilities including 22 memory corruption flaws that can be exploited for arbitrary code execution, a content spoofing flaw, a cross-site request forgery flaw, and an insufficient input validation flaw affecting a Uniform Resource Locator (URL), among other vulnerabilities.
Source: http://www.securityweek.com/adobe-patches-flaws-flash-photoshop-connect

21. *February 9, IDG News Service* – (International) **Google adds warning to unencrypted emails.** Google released a new security feature in its email services that warned users when a recipient's email does not support transport layer security (TLS) encryption and reminded users to be mindful of transmitting or revealing sensitive information via email. The new feature will use a small red unlocked padlock icon to

warn users of the various security levels.
Source: http://www.computerworld.com/article/3031223/security/google-adds-warning-to-unencrypted-emails.html#tk.rss_security

22. *February 9, The Register* – (International) **Sophisticated malware-as-a-racket fraudsters have been scamming businesses for 10 years.** Security researchers from Kaspersky Lab reported that the Poseidon Group, a global cyber-espionage group, has been targeting international financial sectors, telecommunications sectors, critical manufacturing sectors, and energy sectors to collect information from company networks via spear-phishing packages that are embedded with executable elements inside Word documents, and using the information to blackmail victim companies into contracting the Poseidon Group as a security firm. Researchers found that several of the infections were found to have a very short life span which contributed to the malware being undetectable.
Source: http://www.theregister.co.uk/2016/02/09/poseidon_cybercrime_racket/

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. *February 10, Riverside County Press-Enterprise* – (California) **Corona: Bomb scare ends; questions linger about dead man.** Approximately 1,000 people from Parkridge Elementary School, Parkridge Meadows Apartments, and Amberlite mobile home park in Corona were evacuated for more than 8 hours February 9 after a man was found dead in a van parked on a nearby street with a note warning of a bomb and a deadly gas inside the vehicle. Police responded and deemed the area safe after no explosives or evidence of poisonous gas was found.
Source: http://www.pe.com/articles/elementary-793924-bomb-corona.html

24. *February 10, New Rochelle Daily Voice* – (New York) **New Rochelle fire forces 60 onto snowy streets.** A 2-alarm fire at a New Rochelle apartment complex prompted the evacuation of 60 residents and injured 6 people February 10 after the fire began in an apartment unit and spread to surrounding units. Officials are investigating the cause of the fire.
Source: http://newrochelle.dailyvoice.com/police-fire/new-rochelle-fire-forces-60-onto-snowy-streets/624812/

25. *February 9, KTRK 13 Houston* – (Texas) **Three-alarm fire rips through warehouse**

in southwest Houston. A Houston warehouse complex sustained extensive damage February 9 after a 3-alarm fire began in an industrial park and spread to surrounding warehouses, prompting over 100 firefighters to contain the incident. No injuries were reported and officials are investigating the cause of the blaze.
Source: http://abc13.com/news/three-alarm-fire-burning-warehouse-in-southwest-houston/1193428/

26. *February 9, KUSA 9 Denver* – (Colorado) **Greeley fire crews respond to overnight restaurant fire.** A 2-alarm fire at the Country Inn Restaurant in Greeley caused approximately $100,000 in damages after officials reported the incident began due to a structural fire February 9. No injuries were reported.
Source: http://www.9news.com/story/news/local/2016/02/09/greeley-fire-crews-respond-overnight-restaurant-fire/80068958/

27. *February 9, WJXT 4 Jacksonville* – (Florida) **Five arrested in Florida cargo theft ring.** The Jacksonville Sheriff's Office arrested and charged five men for their involvement in a grand theft cargo scheme February 9 after the men allegedly stole $1.2 million worth of merchandise by stealing eight parked semi-trucks from five Florida counties and selling the stolen properties for monetary goods on the black market.
Source: http://www.news4jax.com/news/crime/five-arrested-in-florida-cargo-theft-ring

Dams Sector

28. *February 10, St. Joseph News-Press* – (Missouri) **Local levee finally getting repairs.** U.S. officials announce February 9 that the U.S. Army Corps of Engineers will begin repairing the Missouri River levees as part of the Civil Works program, which requires that $2 million be designated for the levee's repair.
Source: http://www.newspressnow.com/news/local_news/article_a95472af-56c5-584c-9043-512a74ecf464.html

29. *February 8, Worchester Telegram & Gazette* – (Massachusetts) **Quabbin to overhaul power grid, install security cameras.** Massachusetts Water Resource Authority announced February 7 that they would spend $3.2 million over the course of 14 months to upgrade electrical and security equipment at the Quabbin Reservoir by replacing power lines, increasing security measures, and enhancing communications.
Source: http://www.telegram.com/article/20160207/NEWS/160209375

30. *February 7, Kennewick Tri-City Herald* – (Washington) **$8 million upgrades set at Ice Harbor, LoMo dam locks.** The U.S. Army Corps of Engineers awarded contracts worth $8 million February 7 for navigation lock repairs at the Ice Harbor Dam near Burbank and the Lower Monumental Dam near Kahlotus, which are set to begin December 2016 and continue into March 2017.
Source: http://www.tri-cityherald.com/news/local/article59089433.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.