Daily Open Source Infrastructure Report
01 April 2016

Top Stories

- The Atlanta Police Department and the U.S. Secret Service are investigating a half-million dollar credit card fraud operation after they found 366 fraudulent credit cards, multiple credit card-making machines, and $330,000 worth of computers in an Atlanta apartment March 30. – *WSB 2 Atlanta* (See item **8**)
- Cisco released software updates fixing a high severity vulnerability that could allow a remote, unauthenticated attacker to bypass malicious file detection and block security features. – *SecurityWeek* (See item **19**)
- PayPal Holdings, Inc., patched a flaw in one of its automatic emailing application after a security researcher found that attackers could add malicious code to an account's username which were embedded in emails sent to other recipients. – *Softpedia* (See item **22**)
- The Norfolk Admirals Vice President reported that its Admirals system Web site was breached and that 250 users' information was leaked March 30 after a customer was alerted by an identity theft company of potential theft. – *WAVY 10 Portsmouth* (See item **27**)

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. *March 31, Associated Press* – (Georgia) **Energy company halts work on $1 billion Palmetto Pipeline.** Texas-based Kinder Morgan announced March 30 that it suspended work on its Palmetto Pipeline project indefinitely after Georgia lawmakers approved a one-year moratorium on permits for petroleum pipelines in the State. The pipeline is expected to carry gasoline, diesel, and ethanol from South Carolina through Georgia and into Florida.
   Source: http://www.abccolumbia.com/2016/03/31/energy-company-halts-work-on-1-billion-palmetto-pipeline/

2. *March 30, WABC 7 New York City* – (New Jersey) **2 police officers, 3 workers hurt in explosion in Bayonne, NJ.** Three contractors and two police officers were injured when a new Public Service Electric and Gas Company (PSE&G) gas line, which was being tested with pressurized air, failed and caused an explosion in Bayonne March 30. Utility officials stated that a temporary cap blew off under too much air pressure and the incident remains under investigation.
   Source: http://abc7ny.com/news/2-police-officers-3-workers-hurt-in-bayonne-explosion/1268777/

3. *March 30, Associated Press* – (North Dakota) **Regulators: More than 14,000 gallons of saltwater spill.** Cobra Oil and Gas Corp., reported that 14,280 gallons of saltwater was released from a central tank battery, contained, and recovered at a site near Grassy Butte in Billings County March 30.
   Source: http://kfgo.com/news/articles/2016/mar/31/regulators-more-than-14000-gallons-of-saltwater-spill/

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

4. *March 31, Occupational Health and Safety Magazine* – (Washington, D.C.) **Nuclear Security Summit 2016 under way in Nation's capital.** Officials reported that the Nuclear Security Summit 2016 conference will occur March 31 – April 1 with a focus on managing cyber threat and securing the use, storage, and transport of radiological and nuclear materials affecting international nuclear facilities. The conference is the fourth conference in a series of events dating back to 2010.
   Source: https://ohsonline.com/articles/2016/03/31/nuclear-security-summit-under-way.aspx?admgarea=news

5. *March 30, Quincy Patriot Ledger* – (Massachusetts) **Pilgrim reduced to half power for schedule maintenance.** Entergy Corporation reported March 30 that its Pilgrim Nuclear Power Station in Plymouth was operating at half power for an indeterminate amount of time due to a regularly scheduled maintenance procedure.
   Source: http://www.enterprisenews.com/news/20160330/pilgrim-reduced-to-half-

power-for-scheduled-maintenance

Critical Manufacturing Sector

6. *March 30, WBNS 10 Columbus* – (Ohio) **Honda plant in Marysville back open following bomb threat.** A bomb threat at the Honda Motor Company in Marysville, Ohio, prompted the evacuation of approximately 2,000 employees for about 6 hours March 30. Authorities are investigating the incident after the threat was found written on a bathroom wall at the facility.
Source: http://www.10tv.com/content/stories/2016/03/30/marysville-ohio-employees-evacuating-honda-plant-in-marysville-amid-bomb-threat.html

7. *March 30, KXL 101 FM Portland* – (Oregon) **Fire destroys boat building factory in West Linn.** Sixty firefighters responded to a two-alarm fire at Motion Marine in West Linn, Oregon, March 30 that caused significant damage to a building housing manufacturing products such as acetylene, fuel, and ammunition, among other chemicals, as well as boats, chickens, and vehicles. Authorities are investigating the cause of the blaze and the estimated damages.
Source: http://www.kxl.com/fire-boat-building-factory-west-linn/

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

8. *March 30, WSB 2 Atlanta* – (International) **Police bust major credit card fraud operation.** Officials from the Atlanta Police Department and the U.S. Secret Service are investigating a half-million dollar credit card fraud operation after Atlanta police discovered approximately 366 fraudulent credit cards with different numbers, multiple credit card-making machines, and $330,000 worth of computers in an Atlanta apartment March 30. Officials stated the suspects allegedly purchased computers at Best Buy with the fraudulent credit cards and sold the devices internationally, and that they committed fraud using aliases at banks in the U.S., Germany, Denmark, and the Bank of China.
Source: http://www.wsbtv.com/news/local/atlanta/police-bust-major-credit-card-fraud-operation/188069241

9. *March 30, U.S. Department of Justice* – (California) **California wholesale executive pleads guilty for role in $9 million bank fraud scheme.** The former vice president of Eastern Tools and Equipment, Inc., in Ontario, California, pleaded guilty March 30 to Federal charges after he and co-conspirators defrauded East West Bank in Pasadena of $9 million from 2007 – 2012 by making material misrepresentations to the bank about the company's accounts receivable and financial statements, creating shell corporations to act as suppliers and retailers doing business with Eastern Tools, and defaulting on the promissory note issued by the bank. Officials stated that the executive and his co-conspirators prolonged the scheme by opening post office boxes, phone accounts, and

email accounts claiming to be associated with the shell retail companies in order to make them appear as independent entities to East West Bank.
Source: https://www.justice.gov/opa/pr/california-wholesale-executive-pleads-guilty-role-9-million-bank-fraud-scheme

Transportation Systems Sector

10. *March 30, MauiNow.com* – (Hawaii) **Makawao man dies in Haleakala Highway motorcycle crash.** The Haleakala Highway in Pukalani, Maui, was closed for more than 2 hours March 30 while officials investigated the scene of a 2-vehicle crash involving a motorcycle and another vehicle that left 1 driver dead.
Source: http://mauinow.com/2016/03/30/traffic-advisory-haleakala-highway-closed/

11. *March 30, Los Angeles Times* – (California) **Highland Park Gold Line station reopens after suspicious package prompts evacuation.** The Los Angeles County Metro Rail's Gold Line station in Highland Park was shut down for more than 2 hours March 30 due to a suspicious package with a clock on top of it that appeared as a package plugged into an electrical socket at the station. Police investigated and deemed the package safe, allowing service to resume.
Source: http://www.latimes.com/local/lanow/la-me-ln-suspicious-package-highland-park-gold-line-20160330-story.html

For another story, see item **1**

Food and Agriculture Sector

12. *March 31, U.S. Food and Drug Administration* – (National) **Flowers Foods issues allergy alert and voluntary recall on Cobblestone Bread Co. Wheat English Muffins in CT, DE, KY, ME, MD, MA, NH, NJ, NY, NC, OH, PA, RI, SC, TN, VT, VA, DC, and WV.** Flowers Foods, Inc., issued a voluntary recall March 28 for approximately 10,000 packages of its Cobblestone Bread Co., Wheat English Muffin products due to undeclared milk allergens after the company discovered that the packaging did not reveal the presence of milk. No illnesses have been reported and the products were distributed to retail stores in 19 States.
Source: http://www.fda.gov/Safety/Recalls/ucm493484.htm

13. *March 30, U.S. Department of Labor* – (Texas) **OSHA fines nation's largest chicken producer $122k for failures in dangerous ammonia release at Waco plant.** The Occupational Safety and Health Administration cited Pilgrim's Pride Corporation for 2 repeat and 2 serious safety violations March 30 after 79 pounds of anhydrous ammonia was released at the plant in September 2015, endangering workers and prompting an investigation at the Waco, Texas facility which revealed that the company failed to implement proper standard operating procedures with accurate safety information, failed to complete and document equipment testing, and failed to use proper methods to prevent over-pressurization and explosions in the system, among other violations. Proposed penalties total $122,500.
Source:

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=30642

Water and Wastewater Systems Sector

14. *March 31, WFTV 9 Orlando* – (Florida) **Possible sewage leak into Orange County lake.** Crews contained a sewage spill from an underground sewer pipe on Texas Avenue that reached Lake Buchanan in Orange County, Florida, March 29. An investigation into the cause of the leak is ongoing and officials advised the public to avoid the lake until testing for harmful contaminants was completed.
Source: http://www.wftv.com/news/local/sewage-spill-in-lake-buchanan-leads-to-stinky-situation-in-orange-county/187307542

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

15. *March 30, KCBS 2 Los Angeles* – (California) **LA Valley College gets all-clear after 'serious' threats are called in and campus is evacuated.** Evening classes at Los Angeles Valley College in Valley Glen were cancelled March 30 after the campus was evacuated when the school received threats. Officials issued an all-clear after a search revealed no suspicious devices were found.
Source: http://losangeles.cbslocal.com/2016/03/30/la-valley-college-evacuated-after-serious-threats-are-called-in/

16. *March 30, Lexington Herald-Leader* – (Kentucky) **Kentucky State University becomes latest victim of data breach.** Kentucky State University in Frankfort informed current and former university employees March 29 of a March 22 data breach that involved the inadvertent disclosure of personally identifiable information including W-2s for 2015 and university identification information. The university stated that it took action to limit the effects of the breach and is working to identify individuals responsible.
Source: http://www.kentucky.com/news/local/crime/article68960237.html#0

Emergency Services Sector

17. *March 30, Press of Atlantic City* – (New Jersey) **Harborfields juvenile facility evacuated due to fire.** Prisoners at the Harborfields juvenile detention facility in Egg Harbor City were transferred to other facilities after a large dryer caught fire March 30. The fire was contained to the laundry room and no injuries were reported.
Source: http://www.pressofatlanticcity.com/news/harborfields-juvenile-facility-evacuated-due-to-fire/article_f68980ae-f6e5-11e5-b34a-fb565789bd9e.html

18. *March 30, KABC 7 Los Angeles* – (California) **4 firefighters injured in Valley Glen crash involving LAFD fire engine.** Four Los Angeles Fire Department firefighters

were injured when the driver of a fire engine responding to an emergency call suffered a medical emergency and crashed the fire truck into five parked cars in Valley Glen March 30. The fire engine knocked down a pair of power poles which set a store on fire and knocked out power to hundreds of customers in the area.
Source: http://abc7.com/news/4-firefighters-injured-in-valley-glen-crash-involving-lafd-fire-engine/1268693/

Information Technology Sector

19. *March 31, SecurityWeek* – (International) **Malware detection bypass vulnerability found in Cisco firepower.** Cisco released software updates fixing a high severity vulnerability after a researcher found that the flaw was caused by improper input validation of fields in Hypertext Transfer Protocol (HTTP) that could allow a remote, unauthenticated attacker to bypass malicious file detection and block security features by crafting an HTTP request and sending it to the victims' system.
Source: http://www.securityweek.com/malware-detection-bypass-vulnerability-found-cisco-firepower

20. *March 31, The Register* – (International) **Patch out for 'ridiculous' Trend Micro command execution vuln.** Trend Micro released a patch that fixed a command execution vulnerability for systems running its Maximum Security, Premium Security or Password Management software after a security researcher from Google's Project Zero found a remote debugging server was running on customers' machines. Officials stated the patch was not fully complete, but will fix most critical issues with the software.
Source:
http://www.theregister.co.uk/2016/03/31/trend_micro_patches_command_execution_flaw/

21. *March 31, Softpedia* – (International) **XSS and CSRF bugs in Steam Dev panel let anyone be a Valve admin.** A researcher from the United Kingdom discovered a cross-site scripting (XSS) vulnerability and a cross-site request forgery (CSRF) vulnerability affecting SteamDepot, Steam's internal system for storing game content, after finding that a malicious JavaScript code could be added in the description field to steal users' Steam cookies, among other actions.
Source: http://news.softpedia.com/news/xss-and-csrf-bugs-in-steam-dev-panel-lets-anyone-be-a-valve-admin-502394.shtml

22. *March 30, Softpedia* – (International) **Security bug allowed attackers to send malicious emails via PayPal's servers.** PayPal Holdings, Inc., patched a flaw in one of its automatic emailing application after a security researcher from Vulnerability Lab found that attackers could add malicious code to an account's username which were embedded in the emails sent to other recipients. The flaw could allow an attacker to execute session hijacking and redirection to external sources, and trick users into clicking a malicious link that prompts victims to enter their PayPal credentials.
Source: http://news.softpedia.com/news/security-bug-allowed-attackers-to-send-malicious-emails-via-paypal-s-servers-502381.shtml

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

23. *March 30, SecurityWeek* – (International) **New Remaiten malware builds botnet of Linux-based routers.** Security researchers from ESET discovered a new piece of malware dubbed, Remaiten (Linux/Remaiten) has been targeting routers and other embedded Internet of Things (IoT) devices to make the devices part of a botnet controlled by hackers. Researchers found that there were three versions of the malware and each contain several capabilities to infect a device.
Source: http://www.securityweek.com/new-remaiten-malware-builds-botnet-linux-based-routers

Commercial Facilities Sector

24. *March 31, KDVR 31 Denver* – (Colorado) **One injured, 14 displaced in Capitol Hill apartment fire.** The Denver Fire Department reported that a March 30 fire at a Capitol Hill apartment complex caused extensive damage to the facility, injured one person, and displaced 14 others. Firefighters contained the incident and the cause of the fire is under investigation.
Source: http://kdvr.com/2016/03/31/one-injured-14-displaced-in-capitol-hill-apartment-fire/

25. *March 31, WYFF 4 Greenville* – (South Carolina) **17 people displaced following Upstate apartment fire.** A March 30 fire at the Hillcrest Apartment complex in Greenwood, South Carolina, damaged all 8 apartment units and displaced 17 residents after the blaze began in the wall of an apartment unit. A total of five fire departments responded to the incident and the American Red Cross is assisting the displaced residents.
Source: http://www.wyff4.com/news/red-cross-responding-to-upstate-apartment-fire/38767508

26. *March 30, KITV 4 Honolulu; East Idaho News* – (Idaho) **Machete wielding man forces evacuation of Rexburg Idaho Walmart.** The Rexburg Police Chief reported March 30 that a man equipped with a machete and a hammer prompted the evacuation and closure of a Walmart for over two hours after the man entered the facility and allegedly displayed irrational behavior. The man was taken into custody and taken to medical professionals.
Source: http://www.kitv.com/story/31605245/machete-wielding-man-forces-evacuation-of-rexburg-idaho-walmart

27. *March 30, WAVY 10 Portsmouth* – (Virginia) **Norfolk admirals confirm data breach exposing customers' information.** The Norfolk Admirals Vice President reported that its Admirals system Web site was breached and that 250 users' information was leaked March 30 after a customer was alerted by an identity theft company of potential theft. The company stated the breach did not include sensitive credit card or bank account information.
Source: http://wavy.com/2016/03/30/norfolk-admirals-confirm-data-breach-exposing-customers-information/

For another story, see item **18**

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