Homeland Security

Daily Open Source Infrastructure Report
26 March 2013

Top Stories

- Several streets were closed and buildings evacuated in downtown Louisville when an electrical fire caused at least four underground explosions. – *Louisville Courier-Journal* (See item **12**)

- The cause of a diesel fuel spill near Willard Bay State Park remains under investigation after emergency crews removed more than 21,000 gallons of contaminant. – *Associated Press* (See item **16**)

- Forty four individuals were indicted in a health care fraud scheme for allegedly helping bribe physicians and medical professionals in exchange for prescriptions for patients. – *Softpedia* (See item **19**)

- AhnLab stated that the malware that spread through South Korean banking and communications Web sites was distributed via compromised patch management systems. – *The Register* (See item **26**)

Fast Jump Menu

Energy Sector

1. *March 22, WHAM 13 Rochester* – (New York) **Two arrested for copper wire theft.**
   About $32,000 worth of copper wire was stolen from the Dolomite Facility in LeRoy, New York extensively damaging the facility. Police arrested two suspects in connection with the crime the week of March 18.
   Source:
   http://www.13wham.com/news/local/story/copper-dolomite/X_B5vtrAh0W_13uETezo8w.cspx

2. *March 22, Fort Worth Star-Telegram* – (Pennsylvania) **Pennsylvania gas drilling case settled for $750,000.** Fort Worth-based Range Resources along with other defendants settled claims for $750,000 that they disrupted a Pennsylvania family's air and water supply by contaminating the home's surroundings. The family purchased a plot of land to build a home and was not aware the previous owner sold a portion to Range Resources for the purpose of drilling natural gas wells, which in turn contaminated their water and air supply as well as other disturbances.
   Source:
   http://www.star-telegram.com/2013/03/21/4720720/pennsylvania-gas-drilling-case.html

   For additional stories, see items **12**, **16**, and **39**

[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

3. *March 25, Examiner.com* – (National) **Honda recalling 76,000 Acura TSX vehicles from 2004 to 2008.** Honda announced a recall of 76,253 Acura TSX vehicles sold in or currently located in cold weather States due to road salt potentially corroding the vehicles' electronic control units (ECU), creating the potential for stalling.
   Source:
   http://www.examiner.com/article/honda-recalling-76-000-acura-tsx-vehicles-from-2004-to-2008

4. *March 25, Charlottesville Legal Examiner* – (National) **Honda recall 183,000 vehicles due to brake malfunctions.** Honda announced it will recall a total of 183,000 model year 2005 Honda Pilot, Acura MDX, Acura RL vehicles and 800 model year 2006 Acura MDX vehicles due to a problem with their vehicle stability assist (VSA) systems that could cause unexpected braking.
Source:
http://charlottesville.legalexaminer.com/defective-and-dangerous-products/honda-recalls-183000-vehicles-due-to-brake-manfunctions.aspx?googleid=307712

[Return to top]

Defense Industrial Base Sector

See item **23**

[Return to top]

Banking and Finance Sector

5. *March 23, Softpedia* – (International) **Three UK men jailed for stealing millions of euros worth of carbon credits.** Authorities in the United Kingdom sentenced three members of a hacking ring that compromised the Web sites of several financial institutions and illegally transferred about $10 million worth of carbon credits.
Source:
http://news.softpedia.com/news/Three-UK-Men-Jailed-for-Stealing-Millions-of-Euros-Worth-of-Carbon-Credits-339777.shtml

6. *March 23, WABC 7 New York City* – (New York) **4 arrested in alleged debit card scheme.** Four individuals were arrested in New York City for allegedly stealing more than $300,000 using fraudulent debit cards.
Source: http://abclocal.go.com/wabc/story?section=news/local/new_york&id=9038333

7. *March 23, Jersey Journal* – (New Jersey) **Former Kearny councilman charged in $13M mortgage fraud scam.** The FBI arrested and charged a former Kearney councilman for involvement in an alleged mortgage fraud scheme that used straw buyers to obtain $13 million.
Source:
http://www.nj.com/jjournal-news/index.ssf/2013/03/former_kearny_councilman_charg.html

8. *March 22, SC Magazine* – (International) **VSkimmer trojan steals card data on point-of-sale systems.** A new trojan called VSkimmer is capable of infecting Windows systems and stealing financial information from any point of sale (PoS) devices attached to infected systems. VSkimmer appears to be similar to the Dexter PoS malware and to spread via USB devices.
Source:

http://www.scmagazine.com/vskimmer-trojan-steals-card-data-on-point-of-sale-systems/article/285725/

9. *March 22, WAFF 48 Huntsville* – (Alabama; Tennessee) **'Ball Cap Bandit' goes before judge.** The suspect known as the "Ball Cap Bandit" was arrested and held on suspicion of involvement in at least eight bank robberies in Tennessee and northern Alabama. Source: http://www.waff.com/story/21768363/ball-cap-bandit-goes-before-judge

[Return to top]

Transportation Sector

10. *March 25, Richmond Times-Dispatch* – (Virginia) **Snowfall creating messy driving conditions.** The Virginia Department of Transportation reported March 25 over 60 accidents in the Richmond metro area due to a snowstorm.
Source:
http://www.timesdispatch.com/news/latest-news/snowfall-creating-messy-driving-conditions/article_9a38571a-94d4-11e2-97f2-001a4bcf6878.html

11. *March 24, Bristol Herald Courier* – (Virginia) **CSX train derails in Haysi in Dickenson County.** Authorities are investigating a derailment of 18 cars from a CSX train bound for Kentucky that caused four freight cars to plunge into the Russell Fork River in Virginia. Hazmat crews worked to contain a spill from a car containing propionic acid that derailed and started leaking.
Source:
http://www.tricities.com/news/local/article_9106d3ea-93eb-11e2-98cb-0019bb30f31a.html

12. *March 23, Louisville Courier-Journal* – (Kentucky) **Underground fire causes downtown explosions, leave crater in Seventh Street.** Several blocks and streets were evacuated and closed for a number of hours in downtown Louisville when an electrical fire caused at least four underground explosions. The city's police headquarters was also evacuated.
Source:
http://www.courier-journal.com/article/20130323/NEWS01/303230045/Underground-explosions-close-several-blocks-downtown-Louisville

13. *March 23, Associated Press* – (National) **Snowstorm takes aim at Plains, Midwest.** A spring snowstorm caused road closures and canceled flights in Colorado and parts of the Midwest as it moved east March 23.
Source :
http://www.wpxi.com/ap/ap/indiana/snowstorm-takes-aim-at-plains-midwest/nW2w9/

14. *March 21, WCBS 2 New York; Associated Press* – (New Jersey; Delaware; California) **Two shipping firms admit to illegal ocean dumping.** German firm Columbia Shipmanagement and Cyprus-based Columbia Shipmanagement Ltd. settled a plea agreement for $10.4 million after admitting they illegally dumped waste oil and engine

sludge off the coast of Central America from vessels docked in New Jersey, Delaware, and California in 2012.
Source: http://newyork.cbslocal.com/2013/03/22/germany-cyprus-based-shipping-companies-admit-dumping-off-u-s-shores/

For another story, see item **18**

Agriculture and Food Sector

15. *March 25, Food Safety News* – (International) **More smoked salmon recalled in North America for Listeria risk.** Canadian based Central-Epicure Ltd. issued a voluntary recall of its Atlantic Smoked Salmon Friday citing potential Listeria monocytogenes contamination.
Source: http://www.foodsafetynews.com/2013/03/more-smoked-salmon-recalled-for-listeria-risk-in-north-america/#.UVBA7b88zUg

Water Sector

16. *March 24, Associated Press* – (Utah) **Chevron fuel spill in Utah much worse than thought.** The cause of a diesel fuel spill near Willard Bay State Park remains under investigation as estimates were revised from 6,000 gallons of spilled fuel to possibly 27,000 gallons. As of March 22, emergency crews have removed more than 21,000 gallons and estimate up to 6,500 gallons may remain.
Source: http://www.sfgate.com/news/texas/article/Chevron-fuel-spill-in-Utah-much-worse-than-thought-4380552.php

17. *March 21, Boston Globe* – (Massachusetts) **Tugboat spills at least 300 gallons of gear oil.** A tugboat that ran aground spilled at least 300 gallons of gear oil leaving an oil sheen across the southern end of Buzzards Bay. The craft was towed to the Massachusetts Maritime Academy and none of the vessel's 38,000 gallons of fuel spilled.
Source: http://bostonglobe.com/metro/2013/03/21/tugboat-runs-aground-buzzards-bay-spillls-gallons-gear-oil/dLSqk4FN3G0Bg7PJs7G31I/story.html

18. *March 23, Bethesda Patch; Washington Post* – (Maryland) **WSSC lifts water restrictions necessitated by water main break in Chevy Chase.** A 60-inch ruptured main which spilled roughly 60 million gallons of water in Chevy Chase returned to service, although road repairs and work on a nearby stream bed will take weeks to complete. A water restriction request for a reduction in water consumption by 10% that lasted 4 and 1/2 days was also lifted from residents of Montgomery and Prince George's counties.

Source:
http://bethesda.patch.com/articles/wssc-lifts-water-restrictions-necessitated-by-water-main-break-in-chevy-chase

Public Health and Healthcare Sector

19. *March 25, Softpedia* – (National) **US authorities indict 44 for role in healthcare fraud scheme.** Forty four individuals were indicted in a health care fraud scheme for allegedly helping bribe physicians and medical professionals in exchange for prescriptions for patients with private insurance, Medicaid, and Medicare. Pharmacies along with healthcare agency owners were aiding by facilitating the submissions to fake claims to the insurers.
Source:
http://news.softpedia.com/news/US-Authorities-Indict-44-People-for-Role-in-Healthcare-Fraud-Scheme-339887.shtml

Government Facilities Sector

20. *March 24, Associated Press* – (Florida) **Fla. brush fire damages 4 homes.** A Port St. Lucie, Florida wildfire was 90 percent contained March 24 after burning through 120-acres and damaging 4 homes in the area.
Source:
http://www.bradenton.com/2013/03/24/4451646/fla-brush-fire-spreading-quickly.html

21. *March 24, UPI* – (New Jersey) **Bus crash at N.J. base investigated.** A bus crash at the Joint Base McGuire-Dix-Lakehurst military base left 14 military personnel injured when the bus crashed into a car March 23. Authorities are investigating the accident.
Source:
http://www.upi.com/Top_News/US/2013/03/24/Bus-crash-at-NJ-base-investigated/UPI-62131364135293/

22. *March 23, Elmira Star-Gazette* – (New York) **Fire heavily damages Schuyler County shared services building in Watkins Glen.** A building that houses highway department vehicles suffered extensive damage after a fire March 23. Authorities said neighboring towns will aid in vehicle assistance until repairs are made.
Source:
http://www.stargazette.com/article/20130323/NEWS01/303230022/Fire-heavily-damages-Schuyler-shared-services-building?nclick_check=1

23. *March 22, Softpedia* – (National) **Sykipot cybercriminals use new exploits to target government organizations.** Cybercriminals have improved their Sykipot campaign targeting the defense industry and government organizations by setting up fake Web sites that appear to be legitimate government organizations and leading users through malicious

links.
Source:
http://news.softpedia.com/news/Sykipot-Cybercriminals-Use-New-Exploits-to-Target-Government-Organizatons-339540.shtml

For another story, see item **16**

Emergency Services Sector

24. *March 22, Washington Times* – (Washington, D.C.) **D.C. crews face discipline following report.** After a March 21 report indicating that three ambulance crews neglected to respond to an emergency call due to improper monitoring and failing to follow protocols, three Washington, D.C. ambulance crews and a supervisory officer are facing possible disciplinary action.
Source:
http://www.firehouse.com/news/10908991/dc-crews-face-discipline-following-report

25. *March 21, KPHO 5 Phoenix* – (Missouri) **Man allegedly poses as cop to rape woman, police fear more victims.** Kansas City police arrested and charged a man with impersonating a police officer in order to sexually assault a woman. The man pulled over a cab and indicated he was a cop, he then took the woman into his truck and threatened to take her to jail if she did not have relations with him, assaulting her when she refused.
Source: http://www.kpho.com/story/21761304/man-posing-as-police-officer-rapes

For another story, see item **12**

Information Technology Sector

26. *March 25, The Register* – (International) **South Korea data-wipe malware spread by patching system**. South Korean antivirus firm AhnLab stated that the malware that spread through banking and communications Web sites in that country was distributed via compromised patch management systems and delivered to targets as if it were a legitimate software update.
Source: http://www.theregister.co.uk/2013/03/25/sk_data_wiping_malware_latest/

27. *March 25, Threatpost* – (International) **XSS flaw in WordPress plugin allows injection of malicious code.** A vulnerability in the WP Banners Lite plugin for WordPress can allow attackers to inject malicious HTML or Javascript on vulnerable Web sites.
Source:
http://threatpost.com/en_us/blogs/xss-flaw-wordpress-plugin-allows-injection-malicious-code-032513

28. *March 25, Infosecurity* – (International) **Phishers can disguise links with Javascript.** A

researcher disclosed a Javascript method that can be used to show a different URL when a user hovers over a link in a phishing email, disguising the malicious link's destination to appear legitimate.
Source:
http://www.infosecurity-magazine.com/view/31430/phishers-can-disguise-their-links-with-javascript

29. *March 22, Threatpost* – (International) **Command and control used in Sanny APT attacks shut down.** Security firm FireEye and South Korean authorities shut down a compromised message board that was hosting a command and control channel for the Sanny malware campaign.
Source:
http://threatpost.com/en_us/blogs/command-and-control-used-sanny-apt-attacks-shut-down-032213

30. *March 22, Threatpost* – (International) **Apple takes tool offline after new security hole surfaces.** Apple took down its iForgot password reset tool after a vulnerability was discovered that could allow unauthorized access to user accounts.
Source:
http://threatpost.com/en_us/blogs/apple-takes-tool-offline-after-new-security-hole-surfaces-032213

31. *March 22, Symantec* – (International) **New Tidserv variant downloads 50 MB Chromium embedded framework.** A new variant of the Tidserv malware was observed to utilize the legitimate Chromium Embedded Framework (CEF), downloading the framework onto infected systems.
Source:
http://www.symantec.com/connect/blogs/new-tidserv-variant-downloads-50-mb-chromium-embedded-framework

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: https://www.it-isac.org

[Return to top]

Communications Sector

32. *March 23, Allentown Morning Call*– (Pennsylvania) **Police: Men stole $10,000 worth of Verizon utility line.** Two men were charged in Montgomery County with theft, receiving stolen property, and conspiracy for a December 2012 theft of $10,000 worth of copper utility cable after they were spotted by a Verizon utility worker.
Source:
http://www.mcall.com/news/local/police/mc-m-franconia-cable-theft-20130323,0,31607

40.story

33. *March 22, TV News Check* – (Arizona) **KPHO goes dark during March Madness.**
KPHO Phoenix, a CBS affiliate, suffered a transmitter failure which caused the TV station
to be off the air for more than 24 hours.
Source:
http://www.tvnewscheck.com/article/66359/kpho-goes-dark-during-march-madness

[]

Commercial Facilities Sector

35. *March 25, KTLA 5 Los Angeles* – (California) **Beverly Center evacuated over suspicious
package.** A driver alerted police that a briefcase was put in the back seat of his vehicle in a
parking structure prompting an evacuation of the nearby shopping center for several hours
and the detonation of the suspicious package by the Los Angeles Police department police
bomb squad.
Source:
http://ktla.com/2013/03/25/beverly-center-evacuated-over-suspicious-package/#axzz2OY
qsTXYl

36. *March 24, WSYX 6 Columbus* (Ohio) **Altercation leads to shooting outside of club.** A
23-year old male was taken to the hospital for a gunshot wound after a fight inside an after
hour's nightclub led to multiple shots fired at the victim in the club's parking lot.   The
shooter was in police custody.
Source:
http://www.abc6onyourside.com/shared/news/features/top-stories/stories/wsyx_altercatio
n-leads-shooting-outside-club-22903.shtml

37. *March 24, WJBK 2 Detroit* (Michigan) **Three injured after apartment explosion in
Harrison Township.** An explosion at the Beechwood Complex in Harrison Township led
to 3 injuries and the 16-unit building's evacuation while also leaving evidence of drugs and
drug paraphernalia in the wreckage. Members of the Drug Enforcement Agency tested for
evidence of methamphetamine but the results were negative.
Source:
http://www.myfoxdetroit.com/story/21780515/one-injured-after-harrison-township-apart
ment-explosion

38. *March 24, Associated Press* – (Vermont) **10 people displaced in Vt. Apartment building
fire.** Ten people were displaced after an apartment fire in Canaan displaced them and left
heavy damage to the apartment building.
Source:
http://www.ctpost.com/news/article/10-people-displaced-in-Vt-apartment-building-fire-4
380164.php

39. *March 23, WNYT 13, Albany* – (New York) **Underground fire leads to explosion in
downtown Albany.** A March 23 underground electrical problem, the third of its kind in 6

months, led to a fire and explosion in downtown Albany. Surface damage was limited to broken glass and a damaged window sill though officials have become increasingly concerned about the increased danger of electrical explosions and the city's aging infrastructure.
Source: http://wnyt.com/article/stories/S2973741.shtml?cat=300

40. *March 22, Andover American* – (Kansas) **Medical office evacuated.** A Lansing medical office was evacuated and closed for the March 23-24 weekend after people reported a strange odor and experienced health problems. Officials have investigated the issue since March 20, without any readings or additional clues as to the source of the problem.
Source: http://www.andoveramerican.com/article/20130322/NEWS/130329582

41. *March 22, Journal News*– (New York) **Spring Valley condo fire injuries 2, displaces up to 15.** A kitchen fire at a condominium in Spring Valley quickly spread throughout the building and led authorities to evacuate 30 people including 15 people from 4 condo units who would need to find long term alternative housing. Seventy firefighters had the fire under control within 30 minutes but left some to continue investigating and to prevent the fire from flaring up again.
Source: http://www.lohud.com/article/20130322/NEWS03/303220032/

For another story, see item **12**

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

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.