Daily Open Source Infrastructure Report
02 May 2013

Top Stories

- Authorities arrested 18 suspects in connection with a $10 million organized theft ring that allegedly stole and then sold raw copper from an Asarco LLC mine in Hayden, Arizona. – *Phoenix Business Journal* (See item **1**)

- Washington's Chelan County Public Hospital No. 1 was the victim of a cyberattack that moved $1.03 million out of the hospital's payroll system. Organized hackers in Ukraine and Russia performed the attack and used 100 accomplices in the U.S. to move the money. – *Krebs on Security* (See item **23**)

- Two employees at Rawson-Neal Psychiatric Hospital in Las Vegas were fired and 3 were disciplined in an ongoing investigation into the hospital's practice of sending mentally ill patients to other States. – *Sacramento Bee* (See item **24**)

- Researchers found that the U.S. Department of Labor's Web site was infected and used to spread malware the morning of May 1. – *Threatpost* (See item **25**)

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. *April 30, Phoenix Business Journal* – (Arizona) **18 arrested in connection with Arizona copper theft ring.** Authorities arrested 18 suspects in connection with a $10 million organized theft ring that allegedly stole raw copper from an Asarco LLC mine in Hayden. Several workers were charged with helping steal semi-truck loads of copper mined at the site and selling it to metal recyclers throughout the U.S. as well as on the Chinese black market.
Source: http://www.bizjournals.com/phoenix/news/2013/04/30/18-arrested-in-connection-with-arizona.html

2. *April 30, Associated Press* – (Kansas) **Copper theft up: Westar says customers will pay for replacements.** Westar Energy officials determined 31 of their Kansas substations have been hit in April by thieves who caused damage related to copper thefts. The company will replace the stolen copper with materials that have no scrap value and increased costs will eventually be passed on to customers.
Source: http://www.kmuw.org/post/copper-theft-westar-says-customers-will-pay-replacements

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

3. *April 30, Philadelphia Inquirer* – (Pennsylvania) **Three Mile Island to get extra NRC oversight.** The Nuclear Regulatory Commission will increase oversight at the Three Mile Island nuclear power plant in Middletown after it found an issue with flood protection of low to moderate safety significance.
Source:
http://www.philly.com/philly/business/20130501_Three_Mile_Island_to_get_extra_NRC_oversight.html

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

4. *April 30, BankInfoSecurity* – (International) **FBI: DDoS botnet has been modified.** The FBI warned that the Brobot botnet used in a campaign of hacktivist attacks against U.S. banking institutions has been updated in an attempt to circumvent banks' countermeasures.
Source: http://www.bankinfosecurity.com/fbi-ddos-botnet-has-been-modified-a-5719

5. *April 30, Federal Bureau of Investigation* – (California) **Central Coast man pleads guilty to nearly $50 million investment scandal.** A Central Coast man pleaded guilty to running several fraud schemes that caused more than $47 million in losses to victims and banks.
Source: http://www.loansafe.org/central-coast-man-pleads-guilty-to-nearly-50-million-investment-scandal

6. *April 30, Dallas Morning News* – (Texas) **Police seeking information on masked bandit who robbed Arlington bank Monday.** The man who robbed an Arlington, Texas bank April 29 is believed to be the "Mesh Mask Bandit," suspected of robbing 14 other banks in the region since December 2012.
Source: http://crimeblog.dallasnews.com/2013/04/police-seeking-information-on-masked-bandit-who-robbed-arlington-bank-monday.html/

7. *April 30, Laguna Niguel-Dana Point Patch* – (California) **FBI issues bulletin for 'armed and dangerous' bank robber.** A suspect known as the "Gone Plaid Bandit" allegedly robbed a U.S. Bank branch in Los Angeles April 27, and is suspected of robbing 11 total bank robberies in Orange County and surrounding areas.
Source: http://lagunaniguel-danapoint.patch.com/articles/fbi-issues-bulletin-for-armed-and-dangerous-bank-robber-66f54a38

8. *April 30, Federal Deposit Insurance Corporation* – (Pennsylvania) **FDIC orders Citizens Bank of Pennsylvania, Philadelphia, Pennsylvania (CBPA), to pay $5 million for deceptive practices.** The Federal Deposit Insurance Corporation and Citizens Bank of Pennsylvania reached a settlement where the bank will pay a $5 million penalty and $1.4 million in restitution for engaging in deceptive practices that impacted 75,000 consumers.
Source: http://www.loansafe.org/fdic-orders-citizens-bank-of-pennsylvania-philadelphia-pennsylvania-cbpa-to-pay-5-million-for-deceptive-practices

Transportation Systems Sector

9. *May 1, Hagerstown Herald-Mail* – (Maryland) **Man helping to push car on 1-70 is struck, killed; 5 others injured.** The eastbound lanes of Interstate 70 in Washington County were shut down for over 3 hours after a car struck and killed a man and left 5 others injured while he was attempting to assist a disabled vehicle.
Source: http://www.herald-mail.com/news/hm-i70-accident-closes-eastbound-lanes-near-washingtonfrederick-county-line-20130430,0,2016448.story

10. *May 1, Space Coast Daily* – (Florida) **Trucks collide near Port St. John closing I-95.** An accident between two large trucks resulted in 2 people sustaining minor injuries and the partial closure of northbound lanes on Interstate 95 near Port St. John for several hours.
Source: http://spacecoastdaily.com/2013/05/trucks-collide-near-port-st-john-closing-i-95/

11. *May 1, Tallahassee Democrat* – (Florida) **Deerlake principal: Teacher killed in crash was 'enthusiastic' and 'creative.'** A car collided with a bus carrying 43 passengers resulting in one fatality and left 17 others injured as 2 eastbound lanes on Interstate 10 in Leon County were closed for several hours.
Source: http://www.tallahassee.com/article/20130501/NEWS01/130501001/Roadway-now-open-after-fatal-crash-10-eastbound-Video-

12. *April 30, Associated Press* – (California) **Second body found after midair collision over southern California.** A second body was discovered in the Santa Monica Mountains where a small plane crashed and burned after a midair collision April 30.
Source: http://www.huffingtonpost.com/2013/04/30/second-body-found-midair-collision_n_3187304.html

13. *April 30, San Mateo County Times* – (California) **San Francisco man killed in crash on Daly City Freeway.** An accident that resulted in one fatality prompted authorities to close several lanes on Interstate 280 near the Serramonte shopping center in Daly City for nearly 4 hours.
Source: http://www.mercurynews.com/san-mateo-county-times/ci_23139033/man-killed-crash-daly-city-freeway

14. *April 30, La Salle News Tribune* – (Illinois) **Route 351 still closed; repairs expected to last two weeks.** Repair work on the Route 351 bridge in La Salle will take about 2 weeks after heavy flooding damaged the bridge.
Source:
http://newstrib.com/main.asp?SectionID=2&SubSectionID=27&ArticleID=28555

15. *April 30, Associated Press* – (Missouri) **Truck falls on, closes interstate in Kansas City.** A tractor-trailer truck drove over a guardrail and dropped onto Interstate 70 in downtown Kansas City, closing the westbound lanes on the highway for several hours.
Source: http://www.suntimes.com/news/nation/19809238-418/truck-falls-on-closes-

interstate-in-kansas-city.html

Food and Agriculture Sector

16. *April 30, U.S. Food and Drug Administration* – (New York**) Carson's Deli & Bakery issues allergy alert for undeclared allergens in Assorted Cookie Pack and Fudge Brownie Cookie.** Approximately 200 packages of Assorted Cookie Pack and Fudge Brownie Cookies were recalled April 30 by New York-based Carson's Deli & Bakery after it was discovered that the products contain undeclared allergens.
Source: http://www.fda.gov/Safety/Recalls/ucm350276.htm

17. *April 30, U.S. Food and Drug Administration* – (New York**) Prime Food USA issues an alert on Listeria in Latis Brand Herring Fillet "Antalja" in Oil and Latis Brand Herring Fillet in Oil with Spices.** Latis Brand Herring Fillet "Antalja" in Oil and Latis Brand Herring Fillet in Oil with Spices were both recalled by Prime Food USA April 30 due to contamination with Listeria monocytogenes. Both are products of Latvia and were sold throughout New York.
Source: http://www.fda.gov/Safety/Recalls/ucm350268.htm

18. *April 30, Salinas Californian* – (California) **Tainted foods hit California.** The Centers for Disease Control in Atlanta reports that California is the latest State to log a case of illness caused by an outbreak of E. coli 0121 tied to the Rich Products Corp. frozen food products. The company has recalled products for the past 2 months due to the risk of contamination.
Source: http://www.thecalifornian.com/article/20130430/NEWS01/304290023/Tainted-foods-hit-California

Water and Wastewater Systems Sector

19. *May 1, WNCT 9 Greenville* – (North Carolina) **Buncombe Co. sewage leak spills millions of gallons into river.** A pump failure at the Metropolitan Sewage District treatment plant in Woodfin caused millions of gallons of sewage to leak into the French Broad River for several hours before being repaired April 30.
Source: http://www.wnct.com/story/22118349/buncombe-co-sewage-leak-spilling-1m-gallons-per-hour-into-river

20. *April 30, Saginaw News* – (Illinois) **Saginaw Township Wastewater Treatment Plant: 261 million gallons discharged because of heavy rain, river flooding.** More than 8 inches of rain and river flooding caused 261 million gallons of water from the Center Road retention basin in Saginaw to be released into the Tittabawasee River over the course of 3 weeks.
Source:

http://www.mlive.com/news/saginaw/index.ssf/2013/04/saginaw_township_wastewater_tr_6.html

21. *April 29, Charlotte Herald Online* – (South Carolina) **100,000-gallon sewage spill in Tega Cay prompts warning.** The Tega Cay Water Service announced that an April 29, 100,000 gallon partially-treated wastewater spill flowed into Tega Cay cove after the area received 3 inches of rainfall. A no-swimming advisory was issued.
Source: http://www.heraldonline.com/2013/04/30/4818891/100000-gallon-sewage-spill-in.html

Healthcare and Public Health Sector

22. *May 1, WBIR 10 Knoxville* – (Tennessee) **State responding after patient records were discovered at Lakeshore.** A former employee at Lakeshore Mental Health Institute in Knoxville discovered client records at the abandoned building April 30. The institute stopped admitting patients in June 2012 and sent workers to retrieve the documents that dated as far back as 1995.
Source: http://www.wbir.com/news/article/272457/2/Confidential-patient-records-found-in-former-Lakeshore-building

23. *April 30, Krebs on Security* – (Washington) **Wash. hospital hit by $1.03 million cyberheist.** Chelan County Public Hospital No. 1 in Washington was the victim of a $1.03 million breach that moved the money out of the hospital's payroll system. Organized hackers in Ukraine and Russia used a work-at-home scheme to carry out the attack with the help of 100 different accomplices in the U.S.
Source: http://krebsonsecurity.com/2013/04/wash-hospital-hit-by-1-03-million-cyberheist/

24. *April 30, Sacramento Bee* – (Nevada) **Two hospital workers fired over 'dumping' of Nevada psychiatric patients.** Two employees at Rawson-Neal Psychiatric Hospital in Las Vegas were fired and 3 were disciplined in an ongoing investigation into the hospital's practice of sending mentally ill patients to other States. Investigators found that 10 out of nearly 1,500 patients were placed on buses within the last 5 years without proper housing, medication, or contacts once they reached their destinations.
Source: http://www.sacbee.com/2013/04/30/5381856/two-hospital-workers-fired-over.html

Government Facilities Sector

25. *May 1, Threatpost* – (National) **U.S. Department of Labor website discovered hacked, spreading PoisonIvy.** Researchers found that the U.S. Department of Labor's Web site was infected and used to spread malware May 1, though the malware was later removed. The attack collects system information from the victim's computer and

then a malicious payload is downloaded via an Internet Explorer vulnerability, and appeared similar to some previous intelligence-gathering campaigns.
Source: http://www.darkreading.com/attacks-breaches/us-department-of-labor-website-discovere/240153967

26. *April 30, KSTP 5 St. Paul* – (Wisconsin) **Western Wis. elementary school won't reopen after fire.** An April 30 fire at St. Croix Elementary school in Roberts cancelled classes and officials announced the school will be closed for the remainder of the year due to damage throughout the building.
Source: http://kstp.com/news/stories/s3016318.shtml

27. *April 30, Des Moines Register* – (Iowa) **Bomb threat causes evacuation of schools.** Prairie City-Monroe Middle School and Prairie City Elementary School were both evacuated and students and staff were sent home April 30 after a written bomb threat was discovered. Police conducted a search and did not find any explosive devices.
Source: http://www.desmoinesregister.com/article/20130501/NEWS/305010038/-1/MARKETPLACE/Bomb-threat-causes-evacuation-schools

28. *April 30, San Jose Mercury News* – (California) **Marin school gets bomb threat, campus evacuated.** Venetia Valley School in Santa Venetia was evacuated for 3 hours due to a bomb threat that was called in April 30. Police conducted a search and did not find any explosives or suspicious devices.
Source: http://www.mercurynews.com/education/ci_23139977/marin-school-gets-bomb-threat-campus-evacuated

29. *April 30, WXYZ 7 Detroit* – (Michigan) **Sheriff's department, bomb squad respond to Pontiac High School evacuation.** Pontiac High School was evacuated and classes were cancelled April 30 after a student showed a fellow student the interior of his backpack that he claimed held a bomb. The student was in custody after officials cleared the school and searched the student's home and did not find a device.
Source: http://www.wxyz.com/dpp/news/region/oakland_county/sheriffs-department-bomb-squad-respond-to-pontiac-high-school-evacuation

[]

Emergency Services Sector

30. *May 1, WMAQ 5 Chicago* – (Chicago) **3 killed, 20 injured in Chicago gun violence.** April 30-May 1 gun violence in Chicago over the course of 12 hours left 3 dead and 20 wounded, including two teenagers in multiple incidents during the city's first warm day in 7 months.
Source: http://www.nbcchicago.com/news/local/chicago-shootings-205488701.html

For another story, see item **36**

Information Technology Sector

31. *May 1, Softpedia* – (International) **Reputation.com hacked, all users passwords reset.** Internet reputation and management company Reputation.com suffered a security breach where attackers obtained personal information and a limited number of encrypted passwords. The company reset all users' passwords and is investigating. Source: http://news.softpedia.com/news/Reputation-com-Hacked-All-User-Passwords-Reset-350034.shtml

32. *May 1, PCGamesN* – (International) **Not cool: Bitcoin mining malware found in ESEA server client.** The popular ESEA server client used for online gaming was found to contain Bitcoin mining malware, with some users reporting overheated or disabled GPUs as a result of the mining. Source: http://www.pcgamesn.com/counterstrike/not-cool-bitcoin-mining-malware-found-esea-server-client

33. *May 1, Softpedia* – (International) **Cybercriminals register more fake SourceForge domains to distribute trojans.** Researchers have found several fake SourceForge Web sites that were established to spread the ZeroAccess trojan. Source: http://news.softpedia.com/news/Cybercriminals-Register-More-Fake-SourceForge-Domains-to-Distribute-Trojan-349918.shtml

34. *May 1, The Register* – (International) **Mozilla accuses Gamma of dressing up dictators' spyware as Firefox.** Mozilla, the developers of the Firefox browser, filed a cease-and-desist order against Gamma International, developer of the FinFisher intelligence/law enforcement spyware, after the spyware was found imitating the Firefox installer file to infect users' systems. Source: http://www.theregister.co.uk/2013/05/01/mozilla_gamma_cease_and_desist/

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

[Return to top]

Communications Sector

35. *April 30, KFSM 5 Fayetteville* – (Arkansas) **Cox experiences service outages in Northwest Arkansas.** Cox Communications customers in Bentonville and Siloam Springs service areas lost television, Internet, and telephone services April 30 for several hours before the issue was resolved. Source: http://5newsonline.com/2013/04/30/cox-customers-experience-service-

outages-in-northwest-arkansas/

36. *April 29, Big Horn Radio Network* – (Wyoming) **Communications Outage.**
Communications Company Century Link announced that a mile of fiber optics line was damaged and needed to be repaired after a third party cut the fiber optic line April 29, causing a blackout which affected emergency services dispatch centers.
Source: http://www.mybighornbasin.com/Communications-Outage/16220517

[<u>Return to top</u>]

Commercial Facilities Sector

37. *April 30, Department of Labor* – (National) **Waikiki hotel cited by US Department of Labor's OSHA with 14 serious safety and health violations.** The U.S. Department of Labor's Occupational Safety and Health Administration cited Halekulani Corp. owner and operator of Halekulani Hotel in Waikiki Beach, with 14 serious safety violations at the facility, with a total proposed penalty of $49,000.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEAS ES&p_id=24000

38. *April 30, Manhattan Beach Patch* – (California) **Explosion at Mattel Design Center in El Segundo.** A small plastic bottle was believed to be what caused an explosion inside the Mattel Design Center building in El Segundo April 30, and is described as a homemade plastic explosive device. The incident is being investigated by the El Segundo Police Department and the Los Angeles County Sheriff's bomb squad.
Source: http://manhattanbeach.patch.com/articles/explosion-at-mattel-design-center-in-el-segundo

39. *April 30, WMAQ 5 Chicago* – (Illinois) **1 killed, 1 injured in Hyde Park apartment building.** One man was killed and another injured after a gunman entered an apartment building in Chicago's Hyde Park April 29 and opened fire. The murder was the third in as many months in the area.
Source: http://www.nbcchicago.com/news/local/1-Killed-1-Injured-In-Hyde-Park-Apartment-Building-205365181.html

[<u>Return to top</u>]

Dams Sector

Nothing to report

[<u>Return to top</u>]

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.