Daily Open Source Infrastructure Report
23 September 2013

Top Stories

- Researchers identified a watering hole cyberespionage campaign targeting energy sector companies in various parts of the world, a supplier company to nuclear and aerospace companies, and financial services companies that specialize in the energy sector. – *Softpedia* (See item **5**)
- Two Union County, New Jersey women were indicted for allegedly depositing more than $600,000 in counterfeit checks into more than 120 TD Bank accounts and then withdrawing the funds in small amounts. – *Newark Star-Ledger* (See item **10**)
- Researchers discovered a new family of ransomware dubbed CryptoLock which encrypts files important to businesses with AES encryption and demands a ransom to decrypt them. – *Softpedia* (See item **24**)
- An alleged gang-related shooting in a Back of the Yards neighborhood basketball court in Chicago injured 13 people including a young boy. – *USA Today* (See item **30**)

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. *September 19, Associated Press*– (Colorado) **Colorado flooding triggers oil spills, shutdowns.** The Andarko Petroleum Corporation reported a second oil spill of 13,500 gallons along the St. Vrain River near Platteville, following a 5,250 gallons spill in the South Platte River September 18.
   Source: http://www.charlotteobserver.com/2013/09/19/4325970/13500-gallons-of-oil-spill-along.html

2. *September 19, KMSP 9 Minneapolis* – (Minnesota) **Storms push across Minnesota, flooding and power outages reported.** Xcel Energy reported 23,000 customers in the Twin Cities metro area were left without power following heavy area rainfall September 19.
   Source: http://www.myfoxtwincities.com/story/23474681/strong-storms-minnesota-sept-19-2013

3. *September 19, Legal Examiner*– (National) **Halliburton pleads guilty to destruction of evidence regarding oil spill.** Halliburton pleaded guilty in United States federal court September 19 to criminal charges that it destroyed evidence related to the 2010 BP Gulf oil spill and received a $200,000 penalty and probation period of 3 years.
   Source: http://richmond.legalexaminer.com/toxic-substances/halliburton-pleads-guilty-to-destruction-of-evidence-regarding-gulf-oil-spill/

4. *September 19, Network World* – (National) **Energy Department spends $30M to bolster utility cybersecurity tools.** The U.S. Department of Energy awarded 11 security vendors $30 million September 19 to develop technology the agency believes will better protect the nation's electric grid and oil and gas infrastructure from cyberattacks.
   Source: http://www.networkworld.com/news/2013/091913-energy-department-cybersecurity-274005.html

5. *September 19, Softpedia* – (International) **Energy sector companies targeted in watering hole attack, Cisco warns.** Researchers at Cisco identified a watering hole cyberattack campaign targeting energy sector companies in various parts of the world, a supplier company to nuclear and aerospace companies, and financial services companies that specialize in the energy sector. Ten Web sites were compromised by iframe injection and use iframes to load exploit code and malware taking advantage of vulnerabilities in Java, Internet Explorer, Firefox, and Thunderbird.
   Source: http://news.softpedia.com/news/Energy-Sector-Companies-Targeted-in-Watering-Hole-Attack-Cisco-Warns-384511.shtml

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

See item **5**

[Return to top]

Critical Manufacturing Sector

6. *September 20, Car Connection* – (National) **2008-2010 BMW 5-Series & M5 recalled for electrical problem.** BMW annoounced a voluntary recall of 134,100 model year 2008-2010 5-Series and M5 vehicles due to an electrical issue that can cause the rear lights to fail.
   Source: http://www.thecarconnection.com/news/1087073_2008-2010-bmw-5-series-m5-recalled-for-electrical-problem

7. *September 19, U.S. Environmental Protection Agency* – (Arizona) **Asarco agrees to pay $146,000 for PCB violations at Hayden copper smelter.** The U.S. Environmental Protection Agency fined Asarco LLC $30,900 for using buildings contaminated with polychlorinated biphenyls (PCBs) at its copper smelter in Hayden. The company also agreed to spend $115,714 to reduce the amount of PCBs at the facility.
   Source: http://yosemite.epa.gov/opa/admpress.nsf/0/2D134E6EE7E24E4F85257BEB0058E870

For another story, see item **5**

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

8. *September 20, Threatpost* – (International) **FBI warning users about Beta Bot malware.** The FBI warned users about a campaign using the Beta Bot trojan to target online payment systems and financial institutions, as well as blocking users' access to security Web sites and disabling antivirus programs. The malware has been seen propagating via Skype and USB thumb drives
   Source: http://threatpost.com/fbi-warning-users-about-beta-bot-malware

9. *September 19, Orlando Sentinel* – (Florida) **Astatula man charged with $44 million bank fraud.** Federal authorities charged an Astatula man for allegedly using fraudulent information, forged bank statements, and fake tax returns to obtain over $44 million in loans from financial institutions. The man would allegedly obtain loans to pay off previous loans and used the money to make expensive personal purchases.
Source: http://www.orlandosentinel.com/news/local/breakingnews/os-astatula-fraud-benevides-20130919,0,4228840.story

10. *September 19, Newark Star-Ledger* – (New Jersey) **Two Union County women indicted in alleged wide-ranging counterfeit check fraud.** Two women from Union County were indicted for allegedly depositing more than $600,000 in counterfeit checks into more than 120 TD Bank accounts and then withdrawing the funds in small amounts, resulting in $400,000 in losses to the bank.
Source:
http://www.nj.com/union/index.ssf/2013/09/two_union_county_women_indicted_in_alleged_wide-ranging_counterfeit_check_fraud.html

11. *September 19, Macon Telegraph* – (Georgia) **16 former Security Bank officers, directors sued for $21.76 million.** The Federal Deposit Insurance Corporation (FDIC) sued 16 former officers and directors of the failed Security Bank based in Macon for their alleged negligence that led to the failure of the bank. The FDIC is seeking to recover at least $21.76 million.
Source: http://www.macon.com/2013/09/19/2673929/16-former-security-bank-officers.html

For another story, see item **5**

[Return to top]

Transportation Systems Sector

12. *September 19, Associated Press* – (Colorado) **Amtrak's Zephyr train detours due to flooding.** Tracks used by Amtrak's Zephy train are expected to be closed west of Denver through early October on its flood-damaged Moffat Tunnel route. Amtrak will use an alternate route between Denver and Salt Lake City beginning September 20.
Source: http://denver.cbslocal.com/2013/09/19/amtraks-zephyr-train-detours-due-to-flooding/

13. *September 19, WQOW 18 Eau Claire* – (Wisconsin) **Three people injured in crash that shuts down Hwy. 53.** A crash in which three people were injured closed US Route 53 southbound in Altoona for 5 hours September 19.
Source: http://www.wqow.com/story/23478242/2013/09/19/three-people-injured-in-crash-that-shuts-down-hwy-53

14. *September 19, York Daily Record* – (Maryland) **Both lanes open on I-83 southbound**

after crash in Baltimore County. A nine-vehicle crash closed one lane of Interstate 83 southbound in Baltimore County for over 2 hours September 19. Another lane was closed for about 1 hour.
Source: http://www.ydr.com/local/ci_24127050/i-83-southbound-lanes-closed-crash-baltimore-county

[Return to top]

Food and Agriculture Sector

15. *September 20, Food Safety News* – (North Carolina) **Update: 11 Salmonella cases now confirmed, 54 suspected after NC church barbecue.** Health officials in North Carolina announced that there are now 54 probable Salmonella cases, with 11 confirmed, following a fundraising barbecue held September 7 at a church in Shelby.
Source: http://www.foodsafetynews.com/2013/09/nine-salmonella-cases-confirmed-after-church-bbq/

16. *September 19, U.S. Food Safety and Inspection Service* – (California) **California firm recalls ground beef products that may contain foreign materials.** Approximately 58,240 pounds of ground beef was recalled by the Hanford-based Central Valley Meat Company because the products may contain small pieces of plastic.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2013/recall-054-2013-release

17. *September 19, U.S. Food and Drug Administration* – (National) **Wegmans Food Markets issues allergy alert on undeclared soy (allergen) in Wegmans Apple Cinnamon Mini Muffins, 14 oz.** Approximately 4,327 units of Wegmans brand Apple Cinnamon Mini Muffins, 14 ounces, were recalled by Wegmans Food Markets because the products contains undeclared soy.
Source: http://www.fda.gov/Safety/Recalls/ucm369239.htm

[Return to top]

Water and Wastewater Systems Sector

18. *September 19, KXRM 21 Colorado Springs* – (Colorado) **Manitou Springs issues boil water advisory.** A precautionary boil water advisory was issued in Manitou Springs due to a recent flooding and a recent water main break. Officials planned to maintain the advisory until water test results were received September 20.
Source: http://www.fox21news.com/news/story.aspx?id=948841#.UjxhD8akq0g

19. *September 19, Long Island Press*– (New York) **200 gallon fuel spill at Bay park Sewage Plant.** Two hundred gallons of diesel fuel spilled during a delivery run at the Bay Park Sewage Treatment Plant and was contained despite entering a storm drain.
Source: http://www.longislandpress.com/2013/09/19/200-gallon-fuel-spill-at-bay-park-sewage-plant/

[Return to top]

Healthcare and Public Health Sector

Nothing to report

[Return to top]

Government Facilities Sector

20. *September 20, Hartford Courant* – (Connecticut) **Two injured in school bus crash on Route 44 in Canton.** A school bus and another vehicle collided on Route 44 in Canton, Connecticut, September 20, causing minor injuries to two students and two occupants of the vehicle.
Source: http://www.courant.com/community/canton/hc-canton-school-bus-crash-0921-20130920,0,5350772.story

21. *September 20, Yakima Herald-Republic* – (Washington) **School bus crash near Yakima injures 8.** Seven students and a bus driver sustained minor injuries September 19 after a vehicle ran a red light and hit their bus near Yakima.
Source: http://www.yakimaherald.com/photosandvideos/latestphotos/1515749-8/photosvideo-school-bus-crash-near-yakima-injures-8

22. *September 19, Wilmington News Journal* – (Delaware) **Wilmington police: Detonated device was a battery.** The P.S. du Pont Middle School and Harlan Elementary School in Wilmington were locked down for about 3 hours September 19 after a device that turned out to be a battery was unearthed by public works crews.
Source:
http://www.delawareonline.com/article/20130919/NEWS01/309190063/Possible-explosives-found-block-evacuated-Wilmington

[Return to top]

Emergency Services Sector

23. *September 20, Associated Press* – (Wisconsin) **Fire, explosions destroy Wis. fire hall.** The Gordon Fire Hall was destroyed in a fire September 19 along with six fire trucks and firefighting equipment.
Source: http://www.kare11.com/news/article/1039756/396/Fire-explosions-destroy-Wis-fire-hall

[Return to top]

Information Technology Sector

24. *September 20, Softpedia* – (International) **New file encrypting ransomware**

CryptoLocker targets organizations. Emsisoft researchers discovered a new family of ransomware dubbed CryptoLock (or Trojan:Win32/Crilock) which encrypts files important to businesses with AES encryption and demands a ransom to decrypt them. The ransomware appears to be targeting businesses due to the types of files it encrypts and the types of emails used to distribute its downloader.
Source: http://news.softpedia.com/news/New-File-Encrypting-Ransomware-CryptoLocker-Targets-Organizations-384790.shtml

25. *September 19, The Register* – (International) **New ransomware strain forces hapless users into becoming Bitcoin miners.** A new variant of the Reveton ransomware spotted by researchers at Malwarebytes locks out users from their computers and then uses the infected system to mine Bitcoins.
Source: http://www.theregister.co.uk/2013/09/19/bitcoinmining_ransomware/

26. *September 19, Threatpost* – (International) **Apple's iOS 7 update fixes 80 security bugs.** Apple's release of the new version of its mobile operating system, iOS7, fixes several security issues that could be used to bypass security measures, perform denial of service (DoS) attacks, or allow arbitrary code execution.
Source: http://threatpost.com/apples-ios-7-update-fixes-80-security-bugs

For another story, see item **8**

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

27. *September 20, Asbury Park Press*– (New Jersey) **Verizon Wireless outages continue throughout NJ.** Verizon Wireless outages for Ocean County and several other surrounding area Verizon customers lasted several hours beginning September 19. Verizon restored service September 20 and did not report a known cause for the outage.
Source: http://www.app.com/article/20130919/NJNEWS/309190104/

28. *September 19, Taos News*– (New Mexico) **Cell and Internet service restored for Taos residents.** CenturyLink customers in Taos lost cellular and Internet service for 8 hours September 19 before it was restored after a third party construction company damaged a fiber optics cable.
Source: http://www.taosnews.com/news/article_567187f0-2141-11e3-9a24-001a4bcf887a.html

29. *September 19, Staten Island NY 1 New York* – (New York) **Residents cleared to return to SoHo apartment after fears it was unstable.** The New York City Fire Department evacuated a SoHo apartment building September 19 until the building could be inspected by a structural engineer after residents complained of excessive shaking during construction adjacent to the building. The building was later cleared for occupancy.
Source: http://statenisland.ny1.com/content/news/189092/residents-cleared-to-return-to-soho-apartment-after-fears-it-was-unstable

[Return to top]

Commercial Facilities Sector

30. *September 20, USA Today* – (Illinois) **Boy, 3, among 13 injured in Chicago park shooting.** An alleged gang-related shooting in a Back of the Yards neighborhood basketball court in Chicago injured 13 people including a young boy September 19. No deaths were reported.
Source: http://www.usatoday.com/story/news/nation/2013/09/20/chicago-shootings-back-of-the-yards/2841251/

31. *September 19, WMC 5Memphis* – (Tennessee) **22-year-old killed, four others injured in apartment complex shooting.** Officers reported several armed men opened fire at the Birch Leaf Apartments September 18 killing one and wounding four other men.
Source: http://www.wmctv.com/story/23470990/police-at-least-three-people-shot-in

[Return to top]

Dams Sector

Nothing to report

[Return to top]

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