



## Daily Open Source Infrastructure Report 09 April 2013

### Top Stories

- A Virginia lawyer pleaded guilty for her role in a fraud scheme involving fraudulently obtained loans guaranteed by the U.S. Small Business Administration, causing over \$100 million in losses. – *Bloomberg News* (See item [6](#))
- Symantec found that the cybercriminals behind the Shylock banking trojan have added new functions and infrastructure to the malware, expanding its targets and capabilities. – *Threatpost* (See item [9](#))
- Tysons Foods will pay close to \$4 million in fines in a settlement with the federal government over the accidental release of chemicals at Tyson plants in four States that caused injuries, property damage, and one death. – *KFSM 5 Fort Smith* (See item [16](#))
- Researchers discovered an open FTP server that holds the source code for several American Megatrends (AMI) BIOS as well as the private signing key for Unified Extensible Firmware Interface (UEFI) updates, information potentially very valuable in carrying out cyberespionage. – *Softpedia* (See item [31](#))

---

### Fast Jump Menu

#### PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

#### SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

#### SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

#### FEDERAL and STATE

- [Government Facilities](#)
  - [Emergency Services](#)
-

## Energy Sector

1. *April 5, USA Today* – (Arkansas) **Oil spill keeping Ark. residents from homes indefinitely.** Twenty-two homes were evacuated after an ExxonMobil pipeline ruptured March 29 and residents may not be allowed back into their homes for another 2 to 3 weeks. After a week of cleanup efforts, nearly 800,000 gallons of oil and water has been removed from the site and about half the oil in the subdivision has been collected.  
Source: <http://www.usatoday.com/story/news/nation/2013/04/05/arkansas-oil-pipeline-rupture/2057987/>
2. *April 5, Odessa American* – (Texas) **Two dead in Ward County rig explosion.** An April 5 explosion at Anadarko Well in Ward County blew the crew off the well, leaving two dead and three others with severe injuries. The well was shut in by crews on site and authorities are investigating the cause.  
Source: [http://www.oaoa.com/news/business/article\\_2263dd3a-9e67-11e2-8313-0019bb30f31a.html](http://www.oaoa.com/news/business/article_2263dd3a-9e67-11e2-8313-0019bb30f31a.html)

For another story, see item [11](#)

[\[Return to top\]](#)

## Chemical Industry Sector

3. *April 6, Rome News-Tribune* – (Georgia) **Overtaken trailer causes minor chemical spill.** Authorities in Rome, Georgia, spent several hours transferring a corrosive chemical from an overturned Liquid Cargo Inc. tanker to another tanker when a minor leak was detected after the driver turned sharply and flipped the tanker onto its side. A temporary evacuation was ordered for the immediate area while crews stabilized the scene.  
Source: [http://romenews-tribune.com/view/full\\_story/22174139/article-Followup--Overturned-trailer-causes-minor-chemical-spill-?instance=home\\_news](http://romenews-tribune.com/view/full_story/22174139/article-Followup--Overturned-trailer-causes-minor-chemical-spill-?instance=home_news)
4. *April 5, KTXL 40 Sacramento* – (California) **HazMat crews suit up to stop acid leak.** A hazmat team spent several hours cleaning up a railroad car in the Union Pacific Railway in Roseville containing 16,000 gallons of a ferric acid when it started leaking. The tank car's damaged rubber lining led to the acid eating through the steel shell of the tank.  
Source: <http://fox40.com/2013/04/05/hazmat-crews-suit-up-to-stop-acid-leak/>

For another story, see item [16](#)

[\[Return to top\]](#)

## **Nuclear Reactors, Materials, and Waste Sector**

5. *April 6, New York Times* – (International) **Damaged nuclear plant in Japan leaks toxic water.** Around 120 tons of highly contaminated cooling water was estimated to have breached the inner protective lining of a storage pool that services the damaged Fukushima nuclear power plant in Japan.

Source: <http://www.nytimes.com/2013/04/07/world/asia/japan-nuclear-plant-leaks-radioactive-water.html>

[\[Return to top\]](#)

## **Critical Manufacturing Sector**

Nothing to report

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

Nothing to report

[\[Return to top\]](#)

## **Banking and Finance Sector**

6. *April 5, Bloomberg News* – (Virginia) **Virginia lawyer pleads guilty in \$100 million SBA loan fraud.** A Great Falls lawyer pleaded guilty for her role in a fraud scheme involving fraudulently obtained loans guaranteed by the U.S. Small Business Administration, causing over \$100 million in losses.  
Source: <http://www.bloomberg.com/news/2013-04-05/virginia-lawyer-pleads-guilty-in-100-million-sba-loan-fraud-1-.html>
7. *April 5, Federal Bureau of Investigation* – (Virginia) **Former jewelry store owner and loan officer charged in \$20 million mortgage fraud scheme.** Two individuals from Ashburn were charged by a federal grand jury with conspiracy and bank fraud for allegedly running a \$20 million mortgage fraud scheme.  
Source: <http://www.fbi.gov/washingtondc/press-releases/2013/former-jewelry-store-owner-and-loan-officer-charged-in-20-million-mortgage-fraud-scheme>
8. *April 5, WKRC 12 Cincinnati* – (Ohio) **Three men busted for “well-oiled” credit card scheme.** Three men were charged in Hamilton County for their alleged role in a \$150,000 credit card fraud scheme. Around 90 fraudulent cards were found during their arrest.  
Source: <http://www.local12.com/mostpopular/story/Three-Men-Busted-For-Well-Oiled-Credit-Card-Scheme/Ms3ZQnOAIUONIlqSdf8Pfg.csp>

9. *April 5, Threatpost* – (International) **Shylock trojan going global with new features, resilient infrastructure.** Symantec found that the cybercriminals behind the Shylock banking trojan have added new functions and infrastructure to the malware, expanding the banking institutions that it targets and allowing it to steal other passwords and user information.  
Source: [http://threatpost.com/en\\_us/blogs/shylock-trojan-going-global-new-features-resilient-infrastructure-040513](http://threatpost.com/en_us/blogs/shylock-trojan-going-global-new-features-resilient-infrastructure-040513)

For another story, see item [15](#)

[\[Return to top\]](#)

## **Transportation Sector**

10. *April 8, Fairbanks Daily News-Miner* – (Alaska) **Two dead in Parks Highway accident.** A fatal accident left two dead and closed the Parks Highway about 25 miles south of Cantwell, Alaska, for several hours April 7.  
Source: [http://www.newsminer.com/news/local\\_news/two-dead-in-parks-highway-accident-road-closed-until-p/article\\_f08783f0-9fee-11e2-a41d-0019bb30f31a.html](http://www.newsminer.com/news/local_news/two-dead-in-parks-highway-accident-road-closed-until-p/article_f08783f0-9fee-11e2-a41d-0019bb30f31a.html)
11. *April 8, KSWB 69 San Diego* – (California) **Fuel tanker overturns in Mission Valley.** A tanker overturned April 7 and spilled at least 3,000 gallons of flammable liquid prompting authorities to close a busy intersection in Mission Valley through April 8 while crews worked to clean up the site.  
Source: <http://fox5sandiego.com/2013/04/07/fuel-tanker-overturns-in-mission-valley/#axzz2Pt7VydIc>
12. *April 8, Minneapolis Star Tribune* – (Minnesota) **Three killed, five injured in I-94 crash in north Minneapolis.** A fatal accident April 7 that killed three people and left five others injured on a segment of Interstate 94 in north Minneapolis caused the closure of a portion of the highway for several hours.  
Source: <http://www.startribune.com/local/minneapolis/201841371.html?refer=y>
13. *April 8, Cranberry Patch* – (Pennsylvania) **Nearby: Valencia woman killed in Route 8 motorcycle accident.** Pennsylvania Route 8 in Richland Township was shut down for more than 3 hours because of a fatal accident that left one person dead.  
Source: <http://cranberry.patch.com/articles/nearby-valencia-woman-killed-in-route-8-motorcycle-accident>
14. *April 7, WISC 3 Madison* – (Wisconsin) **Homicide charge for driver in Sun Prairie crash.** Authorities shut down an intersection and northbound on-and off- ramps of Highway 151 in Sun Prairie for several hours April 7 because of a fatal accident that left one person dead.  
Source: <http://www.channel3000.com/news/Busy-Sun-Prairie-roads-closed-due-to-accident/-/1648/19654128/-/f37g0/-/index.html>

15. *April 6, Associated Press* – (California) **Police find stolen mail after counterfeit arrests.** Five men were arrested after two of the men used counterfeit bills at a convenience store which triggered a search of their car and home. Investigators discovered a collection of stolen mail from several California cities.  
Source: <http://www.sacbee.com/2013/04/06/5321366/police-find-stolen-mail-after.html>

For another story, see item [18](#)

[\[Return to top\]](#)

## **Agriculture and Food Sector**

16. *April 5, KFSM 5 Fort Smith* – (National) **Tyson fined \$4 million after accidental chemical releases.** Tysons Foods will pay close to \$4 million in fines in a settlement with the federal government over the accidental release of chemicals at Tyson plants in four States that caused injuries, property damage, and one death.  
Source: <http://5newsonline.com/2013/04/05/tyson-fined-4-million-after-accidental-chemical-releases/>
17. *April 4, Washington State Department of Agriculture* – (Washington) **Washington State dairy fined \$17,000 for violating Water Pollution Control Act.** Edaleen Dairy was cited by the Washington Department of Agriculture for two violations of the State's Water Pollution Control Act. The violations carry a fine of \$17,000.  
Source: [http://www.agweb.com/article/washington\\_state\\_dairy\\_fined\\_17000\\_for\\_violating\\_water\\_pollution\\_control\\_act/](http://www.agweb.com/article/washington_state_dairy_fined_17000_for_violating_water_pollution_control_act/)

[\[Return to top\]](#)

## **Water Sector**

18. *April 7, ARLnow.com* – (Virginia) **Water main break closes busy intersection.** An April 6, 12-inch water main break flooded an intersection in Arlington and closed the intersection for several hours.  
Source: <http://www.arlnow.com/2013/04/07/water-main-break-closes-busy-intersection/>

For another story, see item [40](#)

[\[Return to top\]](#)

## **Public Health and Healthcare Sector**

19. *April 7, WTEV 47 Jacksonville* – (Florida) **Riverside Presbyterian Apartment fire displaces dozens of senior citizens.** A fire caused by an electrical malfunction at Riverside Presbyterian Apartments damaged 25 units, flooded hallways, and displaced dozens of senior citizens. Residents were temporarily placed with relatives or put up in

hotels while crews worked to cleanup up the damage.

Source: <http://www.actionnewsjax.com/content/topstories/story/Riverside-Presbyterian-Apartment-fire-displaces/tkIrOos5o0KCOOu7Zrd-5w.csp>

20. *April 5, Associated Press* – (Nebraska) **Omaha police investigating pharmacy burglaries.** Police are searching for 2 men that are suspected of breaking into two Omaha Walgreens April 4 and stealing prescription drugs. The robberies occurred only hours apart.  
Source: <http://www.sfgate.com/news/crime/article/Omaha-police-investigating-pharmacy-burglaries-4411750.php>
21. *April 5, WBTW 13 Florence; U.S. Department of Veterans Affairs* – (South Carolina) **Computer stolen from VA hospital in Columbia held records of 7,400 Veterans.** The William Jennings Bryan Dorn VA Medical Center in Columbia notified 7,405 Veterans of a potential data breach after a laptop went missing from a locked testing lab February 11, and offered a year of free credit reporting to victims while officials continued investigating the incident.  
Source: <http://www.wbtw.com/story/21895692/computer-stolen-from-va-hospital-in-columbia-held-records-of-7400-veterans>

[\[Return to top\]](#)

## **Government Facilities Sector**

22. *April 5, WBBH 20 Fort Myers* – (Florida) **Detectives: Man threatened U.S. President, LCSO.** After sending several emails threatening to kill a Lee County Sheriff's Office deputy, his family, and then threatening the entire department as well as the U.S. President, investigators arrested a man and placed him in jail.  
Source: <http://www.nbc-2.com/story/21894175/detectives-man-threatened-president-obama-sheriffs-office#.UWLSKZPvtKA>
23. *April 5, Marietta Daily Journal* – (Georgia) **Bartow man accused of threatening Cobb judge.** After a two-month investigation, the Cobb County Sheriff's Office arrested a man after allegedly making threats against a Cobb County Superior Court judge over a property dispute. The man was also charged for allegedly sending threatening emails to the Cartersville City School System Board of Education.  
Source: [http://www.mdjonline.com/view/full\\_story/22162570/article-Bartow-man-accused-of-threatening-Cobb-judge](http://www.mdjonline.com/view/full_story/22162570/article-Bartow-man-accused-of-threatening-Cobb-judge)
24. *April 5, Ocala Star-Banner* – (Florida) **Firefighters battle blaze in Ocala National Forest.** Over 150 acres were burned during a brushfire in Ocala National Forest before crews were able to contain the fire April 7. Officials warned that smoke may still be a problem through April 8 while they conduct controlled burns to clear brush.  
Source: <http://www.ocala.com/article/20130407/ARTICLES/130409722?tc=ar>
25. *April 5, MetroWest Daily News* – (Massachusetts) **Fire at Framingham State caused by overheated laptop.** A Framingham State University dorm room fire displaced 373

residents in the North Hall building after heat from a laptop ignited a mattress April 5. The building suffered severe water damage and students will be housed at other dorms until cleanup efforts are completed.

Source: [http://www.metrowestdailynews.com/news/x2082727297/Fire-at-Framingham-State-caused-by-overheated-laptop?zc\\_p=0](http://www.metrowestdailynews.com/news/x2082727297/Fire-at-Framingham-State-caused-by-overheated-laptop?zc_p=0)

26. *April 5, Associated Press* – (Illinois) **1 dead, kids OK in N. Illinois school bus crash.** A driver was killed and several students suffered minor injuries after an elementary school bus crashed into a vehicle and hit another vehicle before flipping onto its side in Wadsworth April 5. Officials are investigating the cause of the accident.

Source: <http://news.yahoo.com/1-dead-kids-ok-n-illinois-school-bus-152340965.html>

[\[Return to top\]](#)

## **Emergency Services Sector**

27. *April 4, Associated Press* – (Texas) **Authorities: Escaped Texas inmates captured.** Two inmates that escaped from Hopkins County Jail in Sulphur Springs were captured April 4 after authorities spent 2 day searching for the pair.

Source: <http://www.usatoday.com/story/news/nation/2013/04/04/escaped-texas-inmates-captured/2054855/>.

[\[Return to top\]](#)

## **Information Technology Sector**

28. *April 8, V3.co.uk* – (International) **Doctor Web hijacks control of BackDoor botnet from criminals.** Antivirus provider Doctor Web took control of the BackDoor.Bulknet.739 botnet and posted an analysis of its composition and effectiveness.

Source: <http://www.v3.co.uk/v3-uk/news/2259913/doctor-web-hijacks-control-of-backdoor-botnet-from-criminals>

29. *April 7, CVG UK* – (International) **Server attack forces Harmonix sites offline.** Video game developer Harmonix took their Web sites offline April 7 after they detected a possible intrusion.

Source: <http://www.computerandvideogames.com/399601/server-attack-forces-harmonix-sites-offline/>

30. *April 6, Softpedia* – (International) **Microsoft fixes DOM XSS vulnerability on Skype.com.** Microsoft closed a DOM-based cross-site scripting (XSS) vulnerability on the Skype Web site during March after a researcher informed the company of it December 2012.

Source: <http://news.softpedia.com/news/Microsoft-Fixes-DOM-XSS-Vulnerability-on-Skype-com-343527.shtml>

31. *April 5, Softpedia* – (International) **FTP server in Taiwan leaks AMI BIOS source**



**code, UEFI signing key.** Researchers discovered an open FTP server that holds the source code for several American Megatrends (AMI) BIOS as well as the private signing key for Unified Extensible Firmware Interface (UEFI) updates, information potentially very valuable in carrying out cyberespionage.

Source: <http://news.softpedia.com/news/FTP-Server-in-Taiwan-Leaks-AMI-BIOS-Source-Code-UEFI-Signing-Key-343426.shtml>

32. *April 5, Ars Technica* – (International) **Bitcoin wallet service Coinbase faces phishing attacks after data leak.** Coinbase, a wallet service for the virtual currency Bitcoin, accidentally exposed user and transaction information on its Web site, leading to phishing attacks against the revealed email addresses.

Source: <http://arstechnica.com/tech-policy/2013/04/bitcoin-wallet-service-coinbase-faces-phishing-attacks-after-data-leak/>

33. *April 5, SC Magazine* – (International) **Android trojan spreads through Cutwail spam botnet.** A large Cutwail botnet has been found spreading an Android trojan dubbed Stels which is capable of gleaning user information and performing functions on infected devices.

Source: <http://www.scmagazine.com/android-trojan-spreads-through-cutwail-spam-botnet/article/287554/>

34. *April 5, V3.co.uk* – (International) **Coca Cola, Credit Suisse and Mercedes-Benz execs caught up in phishing scam.** Webroot researchers found Microsoft Access files from major international companies for sale on underground market Web sites, offering executives' contact information for use in creating more effective phishing attacks.

Source: <http://www.v3.co.uk/v3-uk/news/2259558/coca-cola-credit-suisse-and-mercedesbenz-execs-caught-up-in-phishing-scam>

For another story, see item [9](#)

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto: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 7, Cranberry Patch; Pittsburgh Post-Gazette*– (Pennsylvania) **Phone and internet service outage affecting Cranberry businesses.** A contractor installing a water line for the town of Cranberry April 5 damaged an underground telephone cable, disrupting Internet and phone services for area businesses. Services were expected to be restored by April 7.

Source: <http://cranberry.patch.com/articles/phone-and-internet-service-outage->



## **Commercial Facilities Sector**

36. *April 8, My Ballard* – (Washington) **1 injured in apartment fire on 62<sup>nd</sup> St. in Ballard.** An April 8 fire sparked by unattended candles injured one resident and caused an estimated \$200,000 worth of damages to the multiplex apartment in Seattle.  
Source: <http://www.myballard.com/2013/04/08/1-injured-in-apartment-fire-on-23rd-st-in-ballard/>
37. *April 7, Boston Globe* – (Massachusetts) **Fire damages Garfield Avenue building Revere; 20 people given emergency shelter by Red Cross.** An April 7 one-alarm fire displaced nearly two dozen people and caused \$100,000 in damage to the third floor of the apartment building.  
Source: <http://www.boston.com/metrodesk/2013/04/07/fire-damages-garfield-avenue-building-revere-people-given-emergency-shelter-red-cross/FyGTCVSoVvOMeZWK1XfBhO/story.html> .
38. *April 7, WNBC 4 New York* – (New York) **Teen charged with setting Bronx blaze that displaced families, injured firefighters.** Residents were evacuated from an apartment complex in New York City's Bronx borough April 6 as 150 firefighters fought a three-alarm fire allegedly set by a teenager who lived in the complex.  
Source: <http://www.nbcnewyork.com/news/local/Fire-In-Bronx-Apartment-Building-Displaces-Several-Families-201773721.html>
39. *April 6, WKYT 27 Lexington* – (Kentucky) **Jackson Police make meth bust, apartment evacuated.** A Jackson apartment building was evacuated April 6, leaving a dozen residents to find alternate lodging after police discovered a meth lab in one of the apartments.  
Source: <http://www.wkyt.com/news/headlines/Police-make-meth-bust-apartment-evacuated-201727271.html?ref=271>
40. *April 5, WBIR 10 Knoxville* – (Tennessee) **2 days after evacuation, Maryville apartment residents can return home.** Foothills Crossing Apartment residents evacuated from the 36-unit apartment April 3 due to water cross-contamination received permission to return to their residences April 5 after Maryville city officials received test results indicating the water was now safe. The investigation revealed a cross-connection hazard which could result in contamination of both the City water system and the apartments' water service.  
Source: <http://www.wbir.com/news/article/263116/2/Maryville-apartments-evacuated-over-water-contamination-concerns>
41. *April 5, WCVB 5 Boston* – (Massachusetts) **Waltham office complex evacuated after gas main break.** Several hundred employees were evacuated from an office complex in Waltham for several hours April 5 after a construction crew ruptured a large gas

main while digging.

Source: <http://www.wcvb.com/news/local/metro-west/Waltham-office-complex-evacuated-after-gas-main-break/-/11983044/19634386/-/n3m8oe/-/index.html>

[\[Return to top\]](#)

## **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 <a href="mailto:cikr.productfeedback@hq.dhs.gov">cikr.productfeedback@hq.dhs.gov</a> or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the <a href="#">DHS Daily Open Source Infrastructure Report</a> and follow instructions to <a href="#">Get e-mail updates when this information changes</a> .
Removal from Distribution List:	Send mail to <a href="mailto:support@govdelivery.com">support@govdelivery.com</a> .

---

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@hq.dhs.gov](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://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.