



## Daily Open Source Infrastructure Report 29 August 2016

### Top Stories

- More than 20,000 Indianapolis Power & Light customers in Marion County, Indiana, lost power August 26 following severe storms that moved through the area. – *WRTV 6 Indianapolis* (See item [1](#))
- Sentry Foods issued a recall August 25 for approximately 21,570 pounds of its frozen chicken entrees products sold in 3 variations due to potential contamination with glass or hard plastic fragments. – *U.S. Department of Agriculture* (See item [11](#))
- Apple released an emergency security update for its iOS devices after discovering three zero-day vulnerabilities plaguing iPhones, iPads, and iPod touches that could allow an attacker to compromise a targeted device. – *SecurityWeek* (See item [17](#))
- A Russian cyber-criminal was convicted August 25 after he stole more than 1.7 million credit card numbers from the point-of-sale systems of various businesses, causing 3,700 financial institutions more than \$169 million in losses. – *U.S. Department of Justice* (See item [21](#))

---

### 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. *August 26, WRTV 6 Indianapolis* – (Indiana) **More than 20,000 without power after strong, sudden storms plow through Marion Co.** More than 20,000 Indianapolis Power & Light customers in Marion County, Indiana, lost power August 26 following severe storms that prompted authorities to issue tornado warnings for the area and forced the closure of Eastwood Middle School.  
Source: <http://www.theindychannel.com/news/local-news/more-than-20000-without-power-after-strong-sudden-storms-plow-through-marion-co>

## Chemical Industry Sector

Nothing to report

## Nuclear Reactors, Materials, and Waste Sector

Nothing to report

## Critical Manufacturing Sector

2. *August 25, WBBJ 7 Jackson* – (Tennessee) **Suspect in custody after gunshots at Black & Decker in north Jackson.** A Stanley Black & Decker plant in Jackson, Tennessee, was closed until August 26 after an employee fired shots at multiple vehicles in the facility's parking lot. Officials stated a suspect was arrested and no injuries were reported.  
Source:  
<http://www.wbbjtv.com/2016/08/25/shots-fired-north-jackson-plant/>

## Defense Industrial Base Sector

Nothing to report

## Financial Services Sector

See item [21](#)

## Transportation Systems Sector

3. *August 26, Albany Democrat-Herald* – (Oregon) **Two from Harrisburg die in auto crash.** All Highway 99 West southbound lanes, 1 northbound lane, and Clear Lake Road near Eugene, Oregon, were closed for 3 hours August 25 while officials investigated the scene of a 3-vehicle accident that left 2 people dead.  
Source: [http://democratherald.com/albany/two-from-harrisburg-die-in-auto-crash/article\\_1f214f45-f8c6-553d-b300-b5b865f1c724.html](http://democratherald.com/albany/two-from-harrisburg-die-in-auto-crash/article_1f214f45-f8c6-553d-b300-b5b865f1c724.html)
4. *August 25, Somerville Courier News* – (New Jersey) **East Brunswick pedestrians killed on Route 22 in Bridgewater.** Two pedestrians died August 25 after being struck

- by a vehicle on Route 22 in Bridgewater, New Jersey, prompting the closure of the roadway for several hours while officials investigated the scene.  
Source: <http://www.mycentraljersey.com/story/news/crime/jersey-mayhem/2016/08/25/two-dead-early-morning-bridgewater-accident/89330936/>
5. *August 25, Associated Press* – (Connecticut) **Man dies following five-car crash on Connecticut highway.** Interstate 91 in New Haven, Connecticut, was closed for several hours August 25 while officials investigated the scene of a 5-vehicle crash that left 1 person dead and sent 2 others to an area hospital.  
Source: <http://www.therepublic.com/2016/08/25/ct-fatal-highway-accident/>
  6. *August 25, Astoria Daily Astorian* – (Oregon) **Log truck accident on Hwy 26 results in serious injuries, long road closure.** Highway 26 near Seaside, Oregon, was closed for more than 4 hours August 25 while officials investigated the scene after a semi-truck carrying logs and another vehicle collided, causing the semi-truck to overturn and spill the logs across the roadway. Two people were transported to area hospitals with injuries.  
Source: [http://www.dailyastorian.com/Local\\_News/20160825/log-truck-accident-on-hwy-26-results-in-serious-injuries-long-road-closure](http://www.dailyastorian.com/Local_News/20160825/log-truck-accident-on-hwy-26-results-in-serious-injuries-long-road-closure)
  7. *August 25, Binghamton Press & Sun-Bulletin* – (New York) **No fatalities: Wrecks jam Route 17.** Route 17 in Binghamton, New York, was closed for several hours August 25 while crews worked to clear the wreckage from a 10-vehicle crash involving a semi-truck and 9 other vehicles. No fatalities were reported and nearly a dozen people were transported to an area hospital with injuries.  
Source: <http://www.pressconnects.com/story/news/local/2016/08/25/major-wreck-pileup-closes-route-17/89359778/>
  8. *August 25, WPSD 6 Paducah* – (Kentucky) **US Highway 641 back open after semi crash.** Highway 641 in Calloway County, Kentucky, was closed for several hours August 25 while crews worked to clear the wreckage after a semi-truck transporting 40,000 pounds of dry rice overturned, spilling its load across the roadway. One person was transported to an area hospital.  
Source: <http://www.wpsdlocal6.com/story/32837908/semi-crash-blocking-traffic-on-us-highway-641>
  9. *August 25, WTIC 61 Hartford* – (Connecticut) **Car rollover traps 3 people on I-95 in East Lyme.** Northbound lanes of Interstate 95 in East Lyme, Connecticut, were closed for over 2 hours August 25 while crews worked to free 3 people trapped in a vehicle that overturned.  
Source: <http://fox61.com/2016/08/25/i-95-northbound-closed-in-east-lyme-due-to-crash/>
  10. *August 25, WJZY 46 Belmont* – (North Carolina) **Crews pull driver from overturned tractor trailer on I-85N near Belmont.** Northbound lanes of Interstate 85 in Belmont, North Carolina, were closed for almost 4 hours August 25 while crews worked to free the driver of an overturned semi-truck that went off the roadway and into nearby

woods.

Source: <http://www.fox46charlotte.com/news/local-news/195819131-story>

## **Food and Agriculture Sector**

11. *August 26, U.S. Department of Agriculture* – (Indiana, Pennsylvania, Texas) **Sentry Foods recalls frozen chicken entrées due to possible foreign matter contamination.** Sentry Foods issued a recall August 25 for approximately 21,570 pounds of its frozen chicken entrees products sold in 3 variations due to potential contamination with glass or hard plastic after the firm received consumer complaints stating extraneous materials were found in the products. There have been no confirmed reports of adverse reactions and the products were shipped to retail locations in Indiana, Texas, and Pennsylvania.  
Source:  
<http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-074-2016-release>

## **Water and Wastewater Systems Sector**

12. *August 25, KCRG 9 Cedar Rapids* – (Iowa) **Floodwaters hit wastewater plants, 2 drinking water sources.** The Iowa Department of Natural Resources advised northeastern Iowa residents to avoid contact with floodwaters and use alternative water sources for cooking, drinking, and washing August 25 after severe flooding partially or completely covered wastewater treatment plants in Protivin, Elma, Decora/Freeport, Fort Atkinson, Waucoma, Riceville, and Lansing. Officials stated the floodwaters also affected drinking water supplies at the Cresco County Club in Howard County and Jerico Jo's in Chickasaw County.  
Source: <http://www.kcci.com/news/floodwaters-hit-wastewater-plants-2-drinking-water-sources/41375450>

For another story, see item [13](#)

## **Healthcare and Public Health Sector**

Nothing to report

## **Government Facilities Sector**

13. *August 25, Shelton Patch* – (Connecticut) **CT DEEP temporarily closes Shelton's Indian Well State Park Thursday.** The Connecticut Department of Energy and Environmental Protection closed the swimming area at Indian Well State Park in Shelton and Mashamoquet Brook State Park in Pomfret August 25 due to high bacteria levels in the water.  
Source: <http://patch.com/connecticut/shelton/ct-deep-temporarily-closes-sheltons-indian-well-state-park-thursday>
14. *August 25, KIFI 8 Idaho Falls/KIDK 3 Idaho Falls* – (Idaho) **Winds slowing containment progress on Henry's Creek Fire.** Crews reached 30 percent containment

August 25 of the 52,233-acre Henry's Creek Fire burning near Ririe, Idaho.

Source: <http://www.localnews8.com/news/winds-slowng-down-containment-progress-on-henrys-creek-fire/41371718>

15. *August 25, Idaho Statesman* – (Idaho) **Containment of Cherry Road Fire near Homedale holding at 95 percent.** Crews reached 95 percent containment August 25 of the roughly 35,300-acre Cherry Road Fire burning west of Homedale, Idaho. Officials estimated the fire would be fully contained by August 29.

Source:

<http://www.idahostatesman.com/news/local/environment/fires/article97772137.html>

For another story, see item [1](#)

## Emergency Services Sector

Nothing to report

## Information Technology Sector

16. *August 26, Softpedia* – (International) **New Locky ransomware version delivered as DLL file.** Cyren security researchers discovered that a variant of the Locky ransomware, Zepto received updates and is now installed on infected devices as dynamic-link library (DLL) files, instead of executable (EXE) files. Researchers also found that the DLL file uses a custom packer in order to prevent detection from anti-malware scanners.  
Source: <http://news.softpedia.com/news/new-locky-ransomware-version-delivered-as-dll-file-507646.shtml>
17. *August 26, SecurityWeek* – (International) **Apple issues emergency fix for iOS zero-days: What you need to know.** Apple released an emergency security update for its iOS devices after discovering its iPhone 4s and later, iPad 2 and later, and iPod touch fifth generation and later versions were plagued with three zero-day vulnerabilities, dubbed Trident, including an information leak in the Kernel, a memory corruption bug that could allow an attacker to jailbreak the device and install surveillance software without user knowledge, and a memory corruption bug in the Safari WebKit, which could allow an attacker to execute arbitrary code and compromise the device when a user clicks a link on a specially crafted Website. Researchers found the vulnerabilities were exploited by Pegasus, a high-end surveillance software, and were leveraged in attacks against human rights activists and journalists via a text message phishing campaign.  
Source: <http://www.securityweek.com/apple-issues-emergency-fix-ios-zero-days-what-you-need-know>
18. *August 25, Softpedia* – (International) **PowerShell script steals credentials from IIS config files.** SecureWorks researchers discovered attackers were exploiting already compromised devices to upload and execute a malicious PowerShell script that searches for Microsoft Internet Information Server (IIS) configuration files on the

infected machine, which store credentials for other connection services as connectionStrings in order to steal the access credentials and copy the content to the local /TEMP folder.

Source: <http://news.softpedia.com/news/powershell-script-steals-credentials-from-iis-config-file-507638.shtml>

19. *August 25, Softpedia* – (International) **Security firm releases decrypter for Alma Locker ransomware.** PhishLabs malware analysts released a decrypter for the Alma Locker ransomware family that allows victims to recover their files without paying the ransom after finding the malware's decrypter was susceptible to a Man-in-the-Middle attack, which allowed the researchers to spoof communications from the attackers' command and control (C&C) server in order to gain insight into how the ransomware's decrypter operates.

Source: <http://news.softpedia.com/news/security-firm-releases-free-decrypter-for-alma-locker-ransomware-507613.shtml>

### **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: <http://www.it-isac.org>

## **Communications Sector**

Nothing to report

## **Commercial Facilities Sector**

20. *August 25, Salisbury Daily Times* – (Maryland) **Salisbury Target store reopens after bomb threat.** A Target Corporation store and surrounding businesses in Salisbury, Maryland, were evacuated for several hours August 25 while authorities investigated a bomb threat against the store. Officials deemed the area safe after no explosives were found.

Source:

<http://www.delmarvanow.com/story/news/local/maryland/2016/08/25/salisbury-target-store-subject-bomb-threat/89340688/>

21. *August 25, U.S. Department of Justice* – (International) **Russian cyber-criminal convicted of 38 counts related to hacking businesses and stealing more than two million credit card numbers.** A Russian cyber-criminal was convicted August 25 after he stole than 1.7 million credit card numbers from various businesses from a server he operated in Russia by hacking retail point-of-sale (PoS) systems and installing malware on the servers in order to make fraudulent purchases, causing 3,700 financial institutions more than \$169 million in losses.

Source: <https://www.justice.gov/opa/pr/russian-cyber-criminal-convicted-38-counts-related-hacking-businesses-and-stealing-more-two>

**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 <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.