Daily Open Source Infrastructure Report
07 April 2016

Top Stories

- A minister was convicted April 5 for his role in a nearly $5 million fraudulent tax return scheme where he and a co-conspirator allegedly filed over 2,700 fraudulent tax returns on behalf of church members in Ohio and other States. – *Associated Press* (See item **1**)
- A Kentucky lawyer, a retired administrative law judge, and a psychologist were charged April 5 with committing $600 million in disability fraud by submitting over 2,000 fake medical claims with the U.S. Social Security Administration seeking disability benefits. – *Reuters* (See item **7**)
- State and Federal officials reported April 5 that 21 brokers in the New York metropolitan area were arrested for knowingly recruiting foreign students to the University of Northern New Jersey, a fake institution set up by DHS in 2012. – *New York Times* (See item **10**)
- Adobe reported April 5 that it will be releasing a patch for its Flash Player 21.0.0.197 and its earlier versions April 7 which will address a zero-day vulnerability after malicious attackers were seen actively exploiting the flaw. – *SecurityWeek* (See item **14**)

Fast Jump Menu

Energy Sector

See item **12**

Chemical Industry Sector

See item **12**

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

1. *April 5, Associated Press* – (National) **Minister convicted in $5 million tax scam.** A traveling minister from Arkansas was convicted April 5 for his role in a nearly $5 million fraudulent tax return scheme where he and a co-conspirator allegedly filed over 2,700 fraudulent tax returns on behalf of church members in Ohio and other States after obtaining church members' personal information by claiming to help the members procure government stimulus funds. The minister and co-conspirator took fees from each tax refund while congregants received the balance.
Source: http://www.foxnews.com/us/2016/04/05/minister-convicted-in-5-million-tax-scam.html

2. *April 5, WUSA 9 Washington, D.C.* – (Maryland) **Serial 'bandage' bank bandit.** The FBI announced a search April 5 for a bank robber dubbed the "Bandage" who robbed a Sandy Spring Bank branch in Burtonsville and a Capital One Bank branch in Elkridge April 1. Authorities stated that the man is suspected of robbing seven other banks in Maryland since October 2015.
Source: http://www.wusa9.com/news/local/maryland/wanted-serial-bank-robber-wearing-neckbrace-eyepatch/121283824

Transportation Systems Sector

3. *April 6, WSOC 9 Charlotte* – (North Carolina) **I-85 closed for hours after tractor-trailer crashes into bridge, catches fire.** Emergency crews shut down the northbound lanes of Interstate 85 in Charlotte for several hours while they worked to clear the wreckage from a crash involving an overturned semi-truck that sent two people to the hospital April 6.

Source: http://www.wsoctv.com/news/local/portion-of-i-85-closed-after-tractor-trailer-crashes-catches-fire/199126149

4. *April 5, Walnut Creek Patch* – (California) **Walnut Creek motorcycle crash shuts down I-680 in both directions.** Interstate 680 in Walnut Creek was closed for more than two hours April 5 while crews worked to clear the wreckage from a fatal motorcycle crash that left one person dead.
   Source: http://patch.com/california/walnutcreek/motorcycle-crash-shuts-down-lanes-i-680-both-directions-breaking

5. *April 5, KXJZ 90.9 FM Sacramento* – (California) **US Highway 50 clear at 65th Street after a big rig overturned Tuesday morning.** Three to five lanes of Highway 50 in Sacramento were shut down for more than two hours April 5 while crews worked to clear the wreckage from a multi-vehicle accident involving a semi-truck and several other vehicles.
   Source: http://www.capradio.org/articles/2016/04/05/multiple-car-crash-shuts-down-east-us-highway-50-at-65th/

Food and Agriculture Sector

6. *April 6, U.S. Food and Drug Administration* – (Texas) **Fresh From Texas recalls apple product because of possible health risk.** Fresh From Texas issued a voluntary recall April 5 and ceased the production and distribution of 14 products containing sliced red apples after 2 random samples of the same product indicated the presence of Listeria monocytogenes during internal company testing. The products were distributed to H-E-B Grocery Stores in Texas.
   Source: http://www.fda.gov/Safety/Recalls/ucm494345.htm

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

7. *April 5, Reuters* – (Kentucky; West Virginia) **Three Kentucky men indicted in $600 million federal fraud case.** An indictment unsealed April 5 charged a Kentucky lawyer, a retired administrative law judge, and a psychologist with committing $600 million in disability fraud by submitting over 2,000 fake medical claims with the U.S. Social Security Administration seeking disability benefits. The attorney advertised his services through the Web site MrSocialSecurity.com and routed clients' claims to a regional office in West Virginia where the administrative law judge would assign the cases to himself or have someone else assign them to him.
   Source: http://www.reuters.com/article/us-kentucky-fraud-idUSKCN0X22MM

8. *April 5, Longview Daily News* – (Washington) **260 PeaceHealth patients potentially exposed to hepatitis and HIV.** PeaceHealth St. John Medical Center in Washington notified 260 patients April 4 who were fitted for dental appliances for sleep apnea

between November 2013 and February 2016 that they may have been exposed to hepatitis B, hepatitis C, or HIV after the hospital learned that some steps in the sterilization process may have been skipped when cleaning the instruments. The medical center stated that no affected patients have tested positive and that patients are being offered free testing as a precaution.
Source: http://tdn.com/news/local/peacehealth-patients-potentially-exposed-to-hepatitis-and-hiv/article_167bdac9-3f28-5a39-877d-51baa5b14e65.html

Government Facilities Sector

9. *April 6, Associated Press* – (Oklahoma; Kansas) **Wildfires flare again in Oklahoma, Kansas, threaten towns.** Woods County Emergency Management encouraged about 300 Freedom, Oklahoma residents to evacuate April 5 due to a wildfire that has burned approximately 40 square miles. Kansas officials stated that homes in Riley and Geary counties were evacuated and ordered voluntary evacuations in Alma in Wabaunsee County due to the wildfire threatening the southern edge of the town.
Source: http://abcnews.go.com/US/wireStory/wildfire-flares-oklahoma-threatens-town-38175875

10. *April 5, New York Times* – (New Jersey) **New Jersey University was fake, but Visa fraud arrests are real.** New Jersey officials and U.S. Immigration and Customs Enforcement authorities announced April 5 that 21 brokers in the New York metropolitan area were arrested for knowingly recruiting foreign students, mainly from China and India, to the University of Northern New Jersey, a fake institution set up by DHS in 2012, in order to obtain student visas. The brokers worked with individuals posing as university officials, charged the students fees, and received kickbacks in the scheme which allowed the students to stay in the county and obtain employment.
Source: http://www.msn.com/en-us/news/crime/new-jersey-university-was-fake-but-visa-fraud-arrests-are-real/ar-BBronBp?li=BBnb7Kz

11. *April 5, WDTN 2 Dayton* – (Ohio) **Chemical spill at Ansonia HS sends 9 to hospitals.** A pesticide spill April 5 at Ansonia Local Schools in Ohio caused 7 students and 2 staff members to be transported to area hospitals for respiratory symptoms while 20 – 30 students and staff members were treated on site following an accidental spill of a Bonide brand concentrated fruit tree spray in the school's agricultural department that spread throughout the school. Firefighters spent 5 hours ventilating the building.
Source: http://wdtn.com/2016/04/05/chemical-spill-reported-at-ansonia-hs/

12. *April 5, Lansing State Journal* – (Michigan) **800 gallons of sulfuric acid spilled at MSU power plant.** Approximately 800 gallons of sulfuric acid spilled from a tanker inside the TB Simon Power Plant at Michigan State University in East Lansing April 5, prompting an evacuation when a small amount of the chemical leaked into a basement aisle and into a storm sewer system. Crews worked to clean up the spill, test the air, and return the affected area to a safe condition for workers.
Source: http://www.lansingstatejournal.com/story/news/local/2016/04/05/police-contained-chemical-spill-closes-road-msu-campus/82649002/

Emergency Services Sector

Nothing to report

Information Technology Sector

13. *April 6, Softpedia* – (International) **Windows' Pirrit adware ported to OS X via Qt Framework.** Security researcher from Cybereason discovered that the OSX/Pirrit adware was infecting Apple Mac users for the first time and hijacking users' Web traffic with several ads via the Qt Framework, which allows programmers to write applications that work on Apple Mac devices, Linux systems, and Microsoft Window devices. The malware was seen using several steps to infiltrate a system after a user launches a Pirrit-laced binary.
    Source: http://news.softpedia.com/news/windows-pirrit-adware-ported-to-os-x-via-qt-framework-502637.shtml

14. *April 6, SecurityWeek* – (International) **Adobe to patch actively exploited Flash zero-day.** Adobe reported April 5 that it will be releasing a patch for its Flash Player 21.0.0.197 and its earlier versions April 7 which will address a zero-day vulnerability after malicious attackers were seen actively exploiting the flaws. Customers were advised to ensure their Flash Players were updated to version 21.0.0.182 or later.
    Source: http://www.securityweek.com/adobe-patch-actively-exploited-flash-zero-day

15. *April 5, SecurityWeek* – (International) **New Locky variants change communication patterns.** Researchers from Check Point discovered that Locky, a prominent ransomware family, had changed its distribution mechanism to use JavaScript (.js) attachments for malware distribution and that another Locky variant was included as the malicious payload in the Nuclear exploit kit (EK) with additional communication changes. In addition, FireEye Labs researchers found that the ransomware was increasing its infection rate and surpassing the Dridex spam activities.
    Source: http://www.securityweek.com/new-locky-variants-change-communication-patterns

For another story, see item **16**

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

Communications Sector

16. *April 6, SecurityWeek* – (International) **Quanta routers plagued by many unpatched flaws.** A security researcher discovered more than 20 vulnerabilities in the latest firmware version of Quanta Computer's LTE QDH routers, and several other devices

including QDH, UNE, Mobily, and YooMee 4G routers that can allow an attacker to obtain sensitive information including credentials and configuration data through several flaws including remote code execution, arbitrary file access, a denial-of-service (DoS) vulnerability, and a hardcoded Secure Shell (SSH) server key that can be used to decrypt SSH traffic going through the router. Quanta stated the vulnerabilities in the LTE QDH routers will not be patched since the routers have reached end of life (EOL). Source: http://www.securityweek.com/quanta-routers-plagued-many-unpatched-flaws

Commercial Facilities Sector

17. *April 6, Colorado Springs Gazette* – (Colorado) **Nine families displaced after apartment fire in south Colorado Springs.** A 3-alarm fire at the Quail Cove Apartments in Colorado Springs damaged at least half of the building, displaced 18 residents, and prompted fire crews to remain on site for nearly 3 hours containing the April 5. One firefighter was treated for exhaustion, but no other injuries were reported. Source: http://gazette.com/no-one-hurt-in-three-alarm-apartment-fire-in-south-colorado-springs/article/1573523

18. *April 5, Portland Oregonian* – (Oregon) **2 teenagers accused of vandalizing 3 Hillsboro churches.** A Hillsboro police spokesman reported April 5 that two teenagers were charged for criminal mischief and felony second-degree burglary after the duo broke into three churches in the Hillsboro, Oregon area and vandalized the inside of each facility on March 25 and from April 2 – April 3. Officials deemed the incidents were not hate crimes.
Source:
http://www.oregonlive.com/hillsboro/index.ssf/2016/04/2_teenagers_accused_of_vandali.html

19. *April 5, WSET 13 Lynchburg* – (Virginia) **20 residents displaced after an apartment fire in Lynchburg.** The Lakeside apartments in Lynchburg, Virginia, sustained extensive damage April 5 after a fire displaced 20 residents and damaged 12 apartment units. One person was treated for smoke inhalation and the incident was contained. Source: http://wset.com/news/local/20-residents-displaced-after-an-apartment-fire-in-lynchburg

For another story, see item **1**

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