Daily Open Source Infrastructure Report
18 April 2016

Top Stories

- IBM Security researchers discovered a hybrid trojan, dubbed "GozNym" was similar to the Nymaim dropper and the Gozi financial malware and believed to have stolen millions of dollars from 22 financial institutions in the U.S. and Canada. – *SecurityWeek* (See item **6**)
- A Washington Metropolitan Area Transit Blue Line train stalled in a tunnel near the Rosslyn station in Virginia April 14, leaving between 100 to 200 riders trapped for more than 1 hour. – *WTTG 5 Washington, D.C.* (See item **9**)
- A former owner of Medistat Group Associates in Dallas was convicted April 13 for falsely billing Medicaid and Medicare nearly $375 million after he and 6 other co-conspirators certified 11,000 Medicare beneficiaries through more than 500 home health providers from January 2006 – November 2011. – *Associated Press* (See item **17**)
- Michigan officials reported that 2 men were charged with conspiracy to commit fraud and interstate transportation of stolen goods April 14 after the duo allegedly ordered 193 Apple iPhones, worth $180,000 using Amway's identity. – *Grand Rapids Press* (See item **27**)

Fast Jump Menu

Energy Sector

1. *April 14, Reuters* – (International) **Six years after BP spill, U.S. sets new offshore oil safety rules.** The U.S. Department of the Interior's Bureau of Safety and Environmental Enforcement announced new oil safety rules April 14 which include stricter design requirements and operational procedures for offshore oil and gas operations.
   Source: http://www.reuters.com/article/us-usa-oil-safety-idUSKCN0XB2EM

Chemical Industry Sector

2. *April 14, Boston Globe* – (Massachusetts) **Employee injured in two-alarm fire at chemical plant in Norfolk.** A two-alarm fire at the Camger Chemical Systems in Norfolk, Massachusetts injured one employee and prompted the closure of a surrounding street April 14 after the blaze began in a chemical mixing room where an employee was mixing solutions. The Massachusetts Department of Environmental Protection confirmed there were no environmental threats to the public and the cause of the blaze is under investigation.
   Source: https://www.bostonglobe.com/metro/2016/04/14/person-injured-fire-chemical-plant-norfolk/fwWBJflQyyrbTx4DflGmeP/story.html

Nuclear Reactors, Materials, and Waste Sector

3. *April 14, Associated Press* – (Massachusetts) **Pilgrim nuclear plant to refuel, close in 2019.** Entergy Corp., officials reported April 14 that its Pilgrim Nuclear Power Station in Massachusetts will have a planned refueling outage in 2017, which will push the plant's closure back to May 2019. The plant's planned shutdown was a result of poor market conditions, reduced revenues, and increased operational costs.
   Source: http://turnto10.com/news/local/pilgrim-nuclear-plant-to-refuel-close-in-2019

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

4. *April 14, U.S. Securities and Exchange Commission* – (Vermont) **SEC case freezes assets of ski resort steeped in fraudulent EB-5 offerings.** The U.S. Securities and Exchange Commission charged two owners of Jay Peak Inc., and its eight business partners for conducting a Ponzi-like fraud scheme April 14 after the group misused more than $350,000 million, which was raised through investments and solicited under the EB-5 Immigrant Investor Program by using the funds for personal expenses and other-than-stated purposes while omitting key information and making false statements

to investors in an effort to construct ski resort facilities and a biomedical research facility in Vermont.
Source: https://www.sec.gov/news/pressrelease/2016-69.html

5. *April 14, San Francisco Chronicle* – (California) **9 charged in alleged San Jose car insurance fraud ring.** The Santa Clara County District Attorney's Office reported April 13 that a San Jose body shop manager, his girlfriend, and seven other body shop owners were charged with insurance fraud after the group allegedly made more than $140,000 by filing false insurance claims following the group's fabrication of over 20 vehicle accidents listed under counterfeit names from 2011 – 2015. The group purchased the insurance policies days before each incident and purposely damaged each car to file claims to several insurance company.
Source: http://www.sfgate.com/crime/article/9-charged-in-alleged-San-Jose-car-insurance-fraud-7250094.php

6. *April 14, SecurityWeek* – (International) **Hybrid trojan "GozNym" targets North American banks.** Researchers from IBM Security discovered a hybrid trojan, dubbed "GozNym," which was reported to be similar to the Nymaim dropper and the Gozi financial malware, leverages Nymaim dropper's stealth and persistence while adding trojan capabilities from Gozi's ISFB parts to facilitate fraud via infected Internet browsers. The trojan is believed to have stolen millions of dollars from victims, targeting 22 financial institutions in the U.S. and Canada including banks, credit unions, e-commerce platforms, and retail banking.
Source: http://www.securityweek.com/hybrid-trojan-goznym-targets-north-american-banks

For another story, see item **27**

Transportation Systems Sector

7. *April 15, KSDK 5 St. Louis* – (Missouri) **EB I-44 in Union reopens after semi crash.** Eastbound lanes of Interstate 44 in Union, Missouri, were closed for more than 6 hours April 14 following a chain-reaction crash involving 3 semi-trucks that caught fire. Westbound lanes of the interstate were closed for 2 hours while crews contained the incident.
Source: http://www.ksdk.com/news/local/truck-crash-hazmat-situation-closes-i-44-in-union/133367696

8. *April 15, ABC News* – (West Virginia) **Plane makes emergency landing after bird strike.** A Delta Air Lines flight en route to Tennessee from New York was forced to make an emergency landing April 14 at Yeager Airport in Charleston, West Virginia, after it experienced a bird strike that cracked the windshield.
Source: http://abcnews.go.com/US/plane-makes-emergency-landing-due-bird-strike/story?id=38417522

9. *April 14, WTTG 5 Washington, D.C.* – (Virginia) **Metro train gets stuck in tunnel near Rosslyn, all passengers evacuated safely.** A train on the Washington

Metropolitan Area Transit Authority's Blue Line stalled in a tunnel near the Rosslyn station in Virginia April 14, leaving between 100 to 200 riders trapped for more than 1 hour before officials hauled the train out of the tunnel and evacuated riders. The disabled train was towed from the station.
Source: http://www.fox5dc.com/news/122569415-story

10. *April 14, KMBC 9 Kansas City* – (Missouri) **Highway Patrol investigates fatal crash on I-29 near Platte City.** One person was killed and a section of Interstate 29 near Platte City was closed for approximately 2 hours April 14 following 2 unrelated crashes.
Source: http://www.kmbc.com/news/fatal-crash-closes-stretch-of-i29-near-platte-city/39026642

11. *April 14, Tucson News Now* – (Arizona) **Highway 80 west of Bisbee reopens; was closed because of crash.** State Route 80 west of Bisbee was closed for more than 3 hours April 14 while crews worked to remove a car that went over an embankment.
Source: http://www.tucsonnewsnow.com/story/31727735/highway-80-west-of-bisbee-closed-because-of-car-over-embankment

Food and Agriculture Sector

12. *April 14, U.S. Department of Agriculture* – (National) **Perfect Fit Meals recalls poultry products due to misbranding and undeclared allergen.** Perfect Fit Meals, LLC issued a nationwide recall for approximately 10,455 pounds of its poultry entrees April 14 due to misbranding and undeclared milk allergens after the firm was notified by a retailer that the products were incorrectly labeled and contained other items.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-029-2016-release

13. *April 14, U.S. Food and Drug Administration* – (National) **OLMA-XXI, Inc. recalls Norven herring in oil because of possible health risk.** OLMA-XXI, Inc., issued a recall April 14 for its Norven herring in oil products due to potential contamination with Listeria monocytogenes following testing conducted by the U.S. Food and Drug Administration. The products were sent to distributors and retail locations in 10 States.
Source: http://www.fda.gov/Safety/Recalls/ucm496275.htm

14. *April 14, U.S. Food and Drug Administration* – (National) **Sugarfina issues allergy alert on undeclared peanuts in milk chocolate malt balls.** Sugarfina LLC issued a voluntary recall for 742 units of its Milk Chocolate Malt Balls packaged in 2-inch acrylic cubes due to misbranding and undeclared peanuts after the company discovered that some of its Peanut Butter Malt Balls were mixed in with a batch of its Milk Chocolate Malt Balls. The products were distributed through Internet sales and sold in several States.
Source: http://www.fda.gov/Safety/Recalls/ucm496259.htm

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

15. *April 15, Boston Globe* – (Massachusetts) **Boston Medical Center to pay $1.1 million to resolve fraud charges.** Massachusetts officials announced April 14 that Boston Medical Center agreed to pay $1.1 million to resolve allegations that the hospital and two of its physicians billed Medicare and Medicaid for more units of a cancer drug than were actually used, for services that were covered by other fees, and for submitted claims of outpatient services that were deemed unnecessary. The medical center is auditing its cancer drug usage, has repaid some of the misused funds, and is investigating pre-surgical services billing issues.
Source: https://www.bostonglobe.com/business/2016/04/14/boston-medical-center-pay-for-medicare-medicaid-fraud/9bKyg3e6k3RoE0lhRyBO7M/story.html

16. *April 14, U.S. Department of Labor* – (New Jersey) **OSHA finds Cooper Hospital exposed employees to needle-stick injuries, bloodborne pathogen hazards.** The Occupational Safety and Health Administration issued 9 serious and 6 other-than-serious safety and health violations to Cooper University Hospital in Camden April 14 following an October 2015 inspection prompted by a complaint, which found that the hospital failed to safeguard employees against needle-stick and bloodborne pathogen exposure. Proposed penalties total $55,000.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=31182

17. *April 14, Associated Press* – (Texas) **Jury convicts Texas doctor in biggest home health care fraud.** A doctor and former owner of Medistat Group Associates in Dallas was convicted April 13 for his role in a false claims scheme that billed Medicaid and Medicare nearly $375 million after he and at least 6 other co-conspirators recruited Medicare clients to sign up for home health care services, falsified records to show that nursing services were being rendered, and performed unnecessary home visits and ordered unnecessary medical services. The doctor and co-defendants certified 11,000 Medicare beneficiaries through more than 500 home health providers between January 2006 and November 2011.
Source: http://www.foxnews.com/health/2016/04/14/jury-convicts-texas-doctor-in-biggest-home-health-care-fraud.html

18. *April 14, Associated Press* – (Oklahoma) **Ex-dentist with filthy clinics admits to money laundering.** A former Oklahoma oral surgeon pleaded guilty April 13 to falsely billing Medicaid in 2012 for anesthesia services he did not personally administer and for depositing at least $15,000 in fraudulent billings into a personal account. The former surgeon was ordered to pay nearly $30,000 in restitution and remains under scrutiny for running 2 Tulsa-area clinics that were shut down due to unsanitary conditions.

Source: http://www.foxnews.com/us/2016/04/14/ex-dentist-with-filthy-clinics-admits-to-money-laundering.html

Government Facilities Sector

19. *April 15, WBAL 11 Baltimore* – (Maryland) **Data breach hits Baltimore city workers, official confirms.** Baltimore officials confirmed April 15 that an undisclosed number of current, former, and retired city workers were notified of a potential data breach following the discovery of unauthorized access of employee data April 14, which may have been used to file fraudulent tax returns. Authorities are investigating the potential breach.
Source: http://www.wbaltv.com/news/data-breach-hits-baltimore-city-workers-official-confirms/39037196

20. *April 14, NBC News* – (Washington) **6 kids injured, 2 critically, after truck slams into bus stop in Washington.** Six Cedar River Middle School students were injured when a vehicle crashed into a school bus stop in Maple Valley, Washington, April 14 after the driver reportedly lost control of the vehicle. The driver was arrested and three of the students were transported to an area hospital for treatment.
Source: http://www.nbcnews.com/news/us-news/6-kids-injured-2-critically-after-truck-slams-bus-stop-n556056

21. *April 14, Wrentham Patch* – (Massachusetts) **Bomb threats at 32 Massachusetts schools in 1 day.** Bomb threats made via robocalls April 14 to 32 Massachusetts schools were deemed hoaxes after the schools were placed on temporary lockdown while police searched the campuses for any suspicious items.
Source: http://patch.com/massachusetts/wrentham/bomb-threats-32-massachusetts-schools-1-day-0

Emergency Services Sector

Nothing to report

Information Technology Sector

22. *April 15, SecurityWeek* – (International) **No patches for QuickTime Flaws as Apple ends support on Windows.** ZDI reported that Apple will no longer release security updates for Window versions of QuickTime after a security researcher from Source Incite found a heap corruption vulnerability that could allow an attacker to exploit the flaw for remote code execution (RCE) once a victim accesses a maliciously crafted Web site or file. Apple released instructions on ways to remove QuickTime for Window users and advised users to remove legacy plugins to enhance their personal computer (PC) security.
Source: http://www.securityweek.com/no-patches-quicktime-flaws-apple-ends-support-windows

23. *April 15, Softpedia* – (International) **Google, Microsoft address problems in their**

URL shorteners. An independent security researcher and a professor at Cornell Tech discovered that many Universal Resource Language (URL) shortening services used by Google and Microsoft, employ short random character tokens that can allow an attacker to infiltrate potential private files holding sensitive information using brute-force attacks. The researchers found the flaw after beginning a series of automated scans on Microsoft's 1drv.com and found it exceptionally easy to brute-force its small 6-character URLs.
Source: http://news.softpedia.com/news/google-microsoft-address-problems-in-their-url-shorteners-503007.shtml

24. *April 14, SecurityWeek* – (International) **Clever techniques help malware evade AV engines.** Security researchers from FireEye released a study titled, Ghost in the Endpoint which revealed that various components of malware went undetected for an extended period of time by antivirus programs including a backdoor dubbed "GOODTIMES," which was left undetected due to its disguise as an Excel file (XLSX) while leveraging a Flash Player exploit.
Source: http://www.securityweek.com/clever-techniques-help-malware-evade-av-engines

25. *April 14, Softpedia* – (International) **Lizzard Squad downs Blizzard servers with massive DDoS attacks.** A Blizzard spokesman reported that its European and U.S. servers that host games such as World of Warcraft, Diablo 3, and Starcraft 2 experienced connectivity and latency issues for several hours April 14 following an potential denial of service (DDoS) attack allegedly conducted by Lizard Squad hacking group. Blizzard technical support was working to mitigate the impact of the attacks.
Source: http://news.softpedia.com/news/lizard-squad-downs-blizzard-servers-with-massive-ddos-attacks-502977.shtml

26. *April 14, Softpedia* – (International) **Microsoft issues optional Windows update to fix MouseJack vulnerability.** Microsoft released its monthly security updates addressing several vulnerabilities including a flaw dubbed, MouseJack after security researchers from Bastille found an attacker could spoof data from a wireless device and force the Universal Serial Bus (USB) dongle to send fraudulent instructions to the connected personal computer (PC) and execute malicious actions.
Source: http://news.softpedia.com/news/microsoft-issues-optional-windows-update-to-fix-mousejack-vulnerability-502962.shtml

For another story, see item **6**

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

Nothing to report

Commercial Facilities Sector

27. *April 14, Grand Rapids Press* – (Michigan) **2 indicted in $180,000 iPhone mail fraud scheme.** The U.S. District Court in Grand Rapids, Michigan, reported that 2 men were charged with conspiracy to commit wire fraud, mail fraud, and interstate transportation of stolen goods April 14 after the two allegedly ordered 193 Apple iPhones, worth $180,000 by impersonating Amway's employees and gaining the company's account information, which were later used to intercept packages during FedEx deliveries. Source: http://www.mlive.com/news/grand-rapids/index.ssf/2016/04/2_indicted_in_180000_iphone_ma.html

For another story, see item **4**

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

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.