Daily Open Source Infrastructure Report
14 July 2014

Top Stories

- Researchers with TrapX released a report stating that an undisclosed Chinese manufacturer of handheld scanners used by shipping, logistics, and manufacturing planted malware on the devices as part of a campaign dubbed "Zombie Zero." – *Securityweek* (See item **12**)
- Four adults and 3 children were killed and 9 others were injured July 10 when a 3-alarm fire broke out at a Lowell apartment building and quickly spread due to the lack of a sprinkler system. – *Boston Globe* (See item **28**)
- Police pursued a burglary suspect into a restaurant inside a Dallas strip mall in Cedar Hill July 9 before the man doused himself in gasoline and set himself and an officer on fire then ran into the parking lot. – *KXAS 5 Fort Worth* (See item **29**)
- A July 7 fire that caused between $15 and $20 million in damage to the Residence at Town Square structure under construction in Amarillo was ruled accidental and likely the result of a subcontractor's cutting operation that sparked a fire. – *KVII 7 Amarillo* (See item **31**)

Fast Jump Menu

Energy Sector

1. *July 10, West Virginia MetroNews* – (West Virginia) **Second guilty plea entered in Logan County kickback scheme.** A Logan County man pleaded guilty July 10 to charges connected to his role in a kickback scheme at Arch Coal's Mountain Laurel Mining Complex in West Virginia. He owned and operated Quality Oil which did construction work on the site and paid an estimated $400,000 in illegal kickbacks during a 4-year period.
   Source: http://wvmetronews.com/2014/07/10/second-guilty-plea-entered-in-logan-county-kickback-scheme/

2. *July 10, Bismarck Tribune* – (North Dakota) **PSC Oks natural gas processing plant.** The North Dakota Public Service Commission approved July 10 the production of the Lonesome Creek natural gas processing plant to be located in McKenzie County with an estimated cost of $280 million. Regulators said the plant would help add processing capacity to the State's infrastructure.
   Source: http://bismarcktribune.com/bakken/psc-oks-natural-gas-processing-plant/article_87236446-087b-11e4-859d-001a4bcf887a.html

[Return to top]

Chemical Industry Sector

3. *July 11, U.S. Environmental Protection Agency* – (Mississippi) **EPA orders Hercules Incorporated to perform response actions at its Hattiesburg facility.** The U.S. Environmental Protection Agency ordered Hercules Incorporated to perform response actions in two areas near its Hattiesburg, Mississippi facility and implement interim measures to address the migration of volatile organic compounds from the facility after an inspection revealed the chemicals contaminated groundwater bordering the property. There are no known risks to the public and implementation of the interim measures began the week of July 7.
   Source:http://yosemite.epa.gov/opa/admpress.nsf/596e17d7cac720848525781f0043629e/6dfaae9826328b7c85257d120053b410

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

4. *July 10, Monroe News* – (Michigan) **Diesel fuel leaks at Fermi.** A leak from a gas turbine generator at the Fermi 2 nuclear power plant in Michigan spilled around 2,500 gallons of diesel fuel July 8. The oil spilled into a separator basin and did not reach the ground or water before being contained.
   Source: http://www.monroenews.com/news/2014/jul/09/diesel-fuel-leaks-fermi/

[Return to top]

Critical Manufacturing Sector

5. *July 11, Detroit News* – (National) **Chrysler recalling 895,000 SUVs for fire risks.** Chrysler announced July 11 that it is recalling 895,000 model year 2011-2014 Jeep Grand Cherokee and Dodge Durango vehicles, 651,000 of which are in the U.S., that may have had their vanity mirror or headliner serviced in such a way that wiring could short circuit, posing a fire hazard.
   Source: http://www.detroitnews.com/article/20140711/AUTO0101/307110047/Chrysler-recalling-895-000-SUVs-fire-risks

6. *July 10, WTVF 5 Nashville* – (Tennessee) **Fire breaks out inside Sumner County auto parts plant.** The Unipres USA Inc., auto parts plant in Portland, Tennessee, was evacuated for several hours July 10 after a fire broke out in a metal press. Production continued later in the day after air quality inside the facility was deemed safe.
   Source: http://www.newschannel5.com/story/25988866/employees-evacuated-from-sumner-county-auto-parts-plant

7. *July 10, U.S. Consumer Product Safety Commission* – (National) **Gemini recalls power adaptor/charges due to burn hazard.** Gemini announced a recall of around 31,000 power adaptor/charges given away in promotional giveaways due to the potential for the adaptors to overheat, posting a burn hazard.
   Source: http://www.cpsc.gov/en/Recalls/2014/Gemini-Recalls-Power-Adaptor-Chargers/

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

8. *July 11, IDG News Service* – (International) **Source code for tiny 'Tinba' banking malware leaked.** Researchers with CSIS Security Group reported that the source code for the Tinba, also known as Zusy, banking malware was posted openly on underweb forums, potentially allowing a greater number of attackers to utilize the malware. The malware is capable of interfering in online banking sessions to steal user credentials and has an unusually small code base.
   Source: http://www.computerworld.com/s/article/9249670/Source_code_for_tiny_Tinba_banking_malware_leaked

9. *July 10, Securityweek* – (International) **Shylock malware infrastructure targeted by international authorities.** Law enforcement agencies in the U.S., E.U. and Turkey

along with several security firms conducted a coordinated operation July 8-9 to seize domains and command and control servers used by the Shylock banking malware. The malware, also known as Caphaw, has infected at least 30,000 computers and been in use since 2011.
Source: http://www.securityweek.com/shylock-malware-infrastructure-targeted-international-authorities

10. *July 10, Fort Worth Star-Telegram* – (Texas) **Lake Worth woman says she is the lone 'Wig Bandit'.** A Lake Worth woman who was arrested on a parole violation and drug warrant admitted to being the "Wig Bandit" responsible for seven bank robberies in the Fort Worth area over 6 months between January 30 and June 10.
Source: http://www.star-telegram.com/2014/07/09/5959786/lake-worth-woman-admits-shes-the.html

[Return to top]

Transportation Systems Sector

11. *July 10, KPIX 5 San Francisco* – (California) **Highway 17 near Los Gatos reopens after fatal big-rig crash, major delays still in effect.** One person was killed and seven others injured in a crash on northbound Highway 17 in Santa Clara County July 10 when a semi-truck collided with 10 other vehicles, closing all lanes for nearly 10 hours.
Source: http://sanfrancisco.cbslocal.com/2014/07/10/traffic-gridlock-crawls-by-at-fatal-big-rig-crash-site-on-highway-17-santa-cruz-mountains-near-los-gatos/

12. *July 10, Securityweek* – (International) **Hackers attack shipping and logistics firms using malware-laden handheld scanners.** Researchers with TrapX released a report stating that an undisclosed Chinese manufacturer of handheld scanners used by shipping, logistics, and manufacturing planted malware on the devices as part of a campaign dubbed "Zombie Zero." The malware attacks company networks once the scanner is connected to the victim's wireless network and sends data to a command and control server located at the Lanxiang Vocational School in China.
Source: http://www.securityweek.com/hackers-attack-shipping-and-logistics-firms-using-malware-laden-handheld-scanners

For another story, see item **18**

[Return to top]

Food and Agriculture Sector

13. *July 10, Reuters* – (Wisconsin) **Wisconsin nine-year-old dies trapped in grain bin.** A child that was helping unblock an auger that became stuck and inoperable died when he became trapped inside a grain bin on a Lancaster farm in Grant County July 10.
Source: http://www.reuters.com/article/2014/07/10/us-usa-wisconsin-farming-accident-idUSKBN0FF2MI20140710

14. *July 10, U.S. Department of Labor* – (Ohio) **Workers exposed to grain bin entrapment at Sabina Farmers Exchange.** The Occupational Health and Safety Administration cited Sabina Farmers Exchange Inc., for 3 repeat and 6 serious safety violations at the company's grain bins in Wilmington and Sabina after the agency inspected the facilities following reports that workers entered a grain storage bin while a sweep auger was operating, exposing the them to severe injury and death. Proposed penalties total $50,051.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=26337

[Return to top]

Water and Wastewater Systems Sector

15. *July 11, WTVB 1590 AM Coldwater* – (Michigan) **Partially treated sewage spilled into the St Joseph River in Union City.** 42,000 gallons of partially treated sewage water overflowed into the St. Joseph River in Union City July 8 due to heavy rain that caused a storage pond to overflow. The discharge was stopped by July 9.
Source: http://wtvbam.com/news/articles/2014/jul/10/partially-treated-sewage-spilled-into-the-st-joseph-river-in-union-city/

16. *July 10, Wichita Falls Times Record News* – (Texas) **City warns of rusty water.** The director of Public Works for Wichita Falls stated that some residents may see rusty water for a time as the Cypress Water Treatment Plant is brought back online as water flow is changed as part of a water reuse program. The rusty water still meets State drinking water standards.
Source: http://www.timesrecordnews.com/news/2014/jul/10/rusty_water/

17. *July 10, Newark Star-Ledger* – (New Jersey) **Boil-water advisory in effect for Bloomfield after E.coli discovered in samples.** Bloomfield, New Jersey, was placed under a boil water advisory July 8 after E. coli bacteria was found in the water during sampling July 7. The advisory was expected to last for several days.
Source: http://www.nj.com/essex/index.ssf/2014/07/boil-water_advisory_in_effect_for_bloomfield_after_e_coli_discovered_in_samples.html

[Return to top]

Healthcare and Public Health Sector

Nothing to report

[Return to top]

Government Facilities Sector

18. *July 11, KING 5 Seattle; Associated Press* – (Washington) **Mills Canyon Fire now 19**

percent contained. Firefighters reached 19 percent containment July 11 of the Mills Canyon Fire after burning more than 18,000 acres in Yakima, Washington. Crews also worked to contain two other fires burning in the State, one of which burned several mobile homes and outbuildings before a line was bulldozed around it July 9.
Source: http://www.king5.com/news/local/MIlls-Canyon-Fire-266744411.html

19. *July 11, Associated Press* – (Alabama) **Alabama man charged with threatening president.** Officials arrested an Alabama man and charged him July 3 with threatening the U.S. President after he was accused of making phone calls to the Federal Protective Service and using social media to post threats.
Source: http://www.goerie.com/apps/pbcs.dll/article?AID=/20140711/APN/307119903

20. *July 10, Associated Press* – (Tennessee) **Guns found at teen slaying suspect's home in Tenn.** The Tennessee Bureau of Investigation reported that several weapons were found July 10 at the Lobelville home of a 15-year-old suspect charged with the fatal shooting of a member of the National Guard of the United States at a Tennessee armory July 9.
Source: http://news.msn.com/crime-justice/guns-found-at-teen-slaying-suspects-home-in-tenn

21. *July 10, Associated Press* – (Minnesota) **Blue Mounds State Park to reopen Monday.** The Blue Mounds State Park in Luverne will reopen July 14 after closing June 18 due to flood damage after receiving 11 inches of rain during two storms. The swimming area will remain closed while officials determine how to address the damaged spillway and dam.
Source: http://minnesota.cbslocal.com/2014/07/10/blue-mounds-state-park-to-reopen-monday/

[Return to top]

Emergency Services Sector

22. *July 11, WLBT 3 Jackson; WDBD 40 Jackson* – (Mississippi) **Six injured in Walnut Grove riot.** The sheriff's department in Leake County reported that six people were injured in a riot at the Walnut Grove Correctional Facility in Mississippi July 10. Authorities are investigating the incident which affected two zones.
Source: http://www.msnewsnow.com/story/25993197/riiot-at-walnut-grove-correctional-facility

23. *July 10, Erie Times-News* – (Pennsylvania) **911 outage hits bigger area.** A cut fiber optic cable knocked out landline 9-1-1 service to roughly 3,700 customers in east and west Springfield. Wind Stream Communications notified Erie County of the issue and reported that service would take about 3 hours to restore.
Source: http://www.goerie.com/article/20140710/NEWS02/307109870/911

[Return to top]

Information Technology Sector

24. *July 10, Securityweek* – (International) **Kaspersky Lab details 'versatile' DDoS trojan for Linux systems.** Researchers with Kaspersky Lab reported identifying a Linux distributed denial of service (DDoS) trojan with several modules to add various capabilities. Components of the trojan were identified a Backdoor.Linux.Ganiw.a and Backdoor.Linux.Mayday.f.
Source: http://www.securityweek.com/kaspersky-lab-details-versatile-ddos-trojan-linux-systems

25. *July 10, Softpedia* – (International) **Gmail for iOS poses man-in-the-middle attack risk.** Lacoon researchers found the Gmail app for iOS can leave users vulnerable to man-in-the-middle (MitM) attacks due to the app lacking the certificate pinning feature. This could allow attackers to use a rogue certificate to impersonate the Gmail server and route traffic through their systems.
Source: http://news.softpedia.com/news/Gmail-for-iOS-Poses-Man-in-the-Middle-Risk-450315.shtml

26. *July 10, SC Magazine* – (International) **Kaspersky quickly addresses XSS flaw impacting company website.** Kaspersky Lab closed a cross-site scripting (XSS) vulnerability on one of its Web sites after being notified of the issue by a security researcher, the company reported July 10. There was no indication that the flaw was exploited by attackers.
Source: http://www.scmagazine.com/kaspersky-quickly-addresses-xss-flaw-impacting-company-website/article/360353/

For additional stories, see items **8** and **9** and **12**

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

[Return to top]

Communications Sector

Nothing to report

[Return to top]

Commercial Facilities Sector

27. *July 11, Associated Press; WKMG 6 Orlando* – (Florida) **Officials: Man loses fingertips on Disney ride.** Officials at Walt Disney World's Magic Kingdom

amusement park in Lake Buena Vista closed the Pirates of the Caribbean ride for several hours July 10 after a patron injured his hand and lost two fingertips. The ride was reopened after an inspection confirmed it was safe.
Source: http://news.msn.com/us/officials-man-loses-fingertips-on-disney-ride

28. *July 10, Boston Globe* – (Massachusetts) **Officials: Investigation of Lowell fire that killed 7 begins.** Four adults and 3 children were killed and 9 others were injured July 10 when a 3-alarm fire broke out at a Lowell apartment building and quickly spread due to the lack of a sprinkler system. Authorities are searching for the source of the fire the engulfed the entire building and left dozens of residents displaced.
Source: http://www.boston.com/news/local/massachusetts/2014/07/10/report-people-missing-alarm-lowell-fire/tmrIEbRzZSiKZkiruISVUP/story.html

29. *July 10, KXAS 5 Fort Worth; Associated Press* – (Texas) **Officer-involved shooting in Cedar Hill after man sets himself on fire.** Police pursued a burglary suspect into a restaurant inside a Dallas strip mall in Cedar Hill July 9 before the man doused himself in gasoline and set himself and an officer on fire then ran into the parking lot. Two additional police officers attempted to restrain the man and were burned before one of the officers shot and wounded the man.
Source: http://www.nbcdfw.com/news/local/Officer-Involved-Shooting-in-Cedar-Hill-After-Man-Sets-Himself-on-Fire-266487591.html

30. *July 10, WBAL 10 Baltimore* – (Maryland) **Child killed, others hurt during storm at Carroll County camp.** High winds associated with a strong storm system downed a tree that struck and killed one child who became trapped under the tree, and injured eight others while they were hiking on a path at the River Valley Ranch in Carroll County July 8.
Source: http://www.wbaltv.com/news/several-people-hurt-at-carroll-county-camp/26853586

31. *July 9, KVII 7 Amarillo* – (Texas) **Fire Marshal determines cause of Town Square Village fire.** Fire officials announced July 9 that a July 7 fire that caused between $15 and $20 million in damage to the Residence at Town Square structure under construction at Town Square Village in Amarillo was ruled accidental and was likely the result of a subcontractor's cutting operation that sparked a small fire.
Source: http://www.connectamarillo.com/news/story.aspx?list=195065&id=1068030

[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