Daily Open Source Infrastructure Report
08 June 2016

Top Stories

- Officials issued a recall the weekend of June 4 for nearly 563,000 model years 2004 – 2011 vehicles in 5 makes sold in the U.S. due to potentially faulty Takata Corp., passenger-side air bag inflators. – *TheCarConnection.com* (See item **3**)
- A former University of Missouri-Columbia administrative officer pleaded guilty June 6 to embezzling over $716,000 from the school over the course of 9 years. – *St. Louis Post-Dispatch* (See item **12**)
- Akamai released a report titled State of the Internet which revealed that during the first quarter of 2016, there were 19 distributed denial-of-service (DDoS) attacks that exceeded 100 Gigabits per second, making DDoS attacks four times more prevalent than the previous quarter. – *IDG News Service* (See item **14**)
- Security researchers from FireEye reported that the Angler exploit kit (EK) installations were capable of bypassing Microsoft's Enhanced Mitigation Experience Toolkit (EMET) on Windows 7 to deliver a malicious payload. – *Softpedia* (See item **15**)

Fast Jump Menu

Energy Sector

See item 7

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

1. *June 7, Allentown Morning Call* – (Pennsylvania) **Water leak forces shutdown of Susquehanna reactor Unit 1.** Talen Energy Corp. officials reported June 6 that its Unit 1 nuclear reactor at the Susquehanna Steam Electric Station in Salem Township was shut down June 5 due to a water leak that occurred on the seal of a reactor recirculation pump. Officials were unsure when Unit 1 would be restored to normal operations, but stated Unit 2 continued to operate at full power.
   Source: http://www.poconorecord.com/article/20160607/NEWS/160609692

2. *June 6, London Platts* – (Tennessee) **TVA's Watts Bar-2 nuclear unit shuts soon after connecting to grid.** Tennessee Valley Authorities reported June 6 that its Unit 2 nuclear reactor at the Watts Bar Nuclear Generating Station in Spring City shut down after the unit experienced turbine system issues June 5. The Federal power producer was working to fix the issue, but officials were unsure when the unit would resume normal operations.
   Source: http://www.platts.com/latest-news/electric-power/washington/tvas-watts-bar-2-nuclear-unit-shuts-soon-after-21634906

Critical Manufacturing Sector

3. *June 6, TheCarConnection.com* – (National) **Even more Takata recalls: 563,000 Audi, BMW, Jaguar, Land Rover, Mercedes-Benz vehicles affected.** The National Highway Traffic Safety Administration issued a recall the weekend of June 4 for nearly 563,000 model years 2004 – 2011 vehicles in 5 makes sold in the U.S. due to potentially faulty Takata Corp., passenger-side air bag inflators equipped with ammonium nitrate, a chemical that may destabilize over time when exposed to hot, humid weather and cause the airbags to deploy with excessive force, spraying hot shrapnel into vehicle passenger compartments. The recalls are being conducted by region, with vehicles registered or sold in the Gulf Coast region taking priority.
   Source: http://www.thecarconnection.com/news/1104320_even-more-takata-recalls-563000-audi-bmw-jaguar-land-rover-mercedes-benz-vehicles-affected

4. *June 6, Help Net Security* – (International) **Researchers hack the Mitsubishi Outlander SUV, shut off alarm remotely.** Pen Test Partners discovered several vulnerabilities in Mitsubishi Motor Corporation's Outlander vehicle's setup including an easy-to-crack pre shared key for the vehicle's Wi-Fi, and predictable format in the vehicle's Wi-Fi Service Set Identifier (SSID) which could allow attackers to easily break into the vehicle remotely via an app, and disable the car's anti-theft alarm, among

other privileges, thereby potentially exposing the vehicle to more attacks. Mitsubishi is working to repair the firmware and advised vehicle owners to deactivate the vehicle's Wi-Fi.
Source: https://www.helpnetsecurity.com/2016/06/06/researchers-hack-mitsubishi-outlander/

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

Nothing to report

Transportation Systems Sector

5. *June 7, Westerly Sun* – (Connecticut) **Tractor-trailer crash on I-95 wreaks havoc on traffic.** Officials closed Interstate 95 South in North Stonington June 6 for more than 7 hours while State officials worked to clear debris and fluid spills from a two-vehicle crash involving a semi-truck and another vehicle.
Source: http://www.thewesterlysun.com/news/policecourts/8930687-154/i-95-southbound-reopened-after-tractor-trailer-crash.html

6. *June 6, USA Today* – (Wisconsin) **1 dead, 2 hospitalized in State 97 crash.** A head-on crash involving three vehicles shut down State Route 97 in Stratford for several hours, sent two people to the hospital with injuries, and left one person dead June 6.
Source: http://www.marshfieldnewsherald.com/story/news/2016/06/06/3-vehicle-crash-near-stratford/85524958/

7. *June 6, KIRO 7 Seattle* – (Oregon) **Oil train derailment focuses on condition of track.** Union Pacific reported that oil trains began their normal operations June 6 in Moiser, Oregon, after being shut down the weekend of June 4 when oil tankers derailed and caught fire due to possible fastener failures June 3.
Source: http://www.kiro7.com/news/local/oil-train-derailment-focuses-on-condition-of-track/326982485

Food and Agriculture Sector

8. *June 7, WVLT 8 Knoxville* – (National) **Salmonella outbreak linked to live poultry includes cases in Tennessee and Kentucky.** The U.S. Centers for Disease Control and Prevention reported June 7 that a total of 324 people in 35 States have been infected by separate outbreaks of Salmonella between January and May. Health officials stated that the outbreak is linked to contact with live poultry in backyard flocks.
Source: http://www.local8now.com/content/news/CDC-investigating-Salmonella-Outbreak-382065091.html

9. *June 6, U.S. Food and Drug Administration* – (National) **Atkins Nutritionals, Inc.**

issues voluntary recall of certain products after sunflower seed supplier expands recall due to Listeria concerns. Atkins Nutritionals, Inc., issued a voluntary recall June 3 for 11 of its bar products that contain sunflower seeds or may have come in contact with equipment that processes the seeds after the company's sunflower seed supplier, SunOpta, Inc., expanded a recall for the seeds it provided the firm due to a potential Listeria monocytogenes contamination. No illnesses have been reported.
Source: http://www.fda.gov/Safety/Recalls/ucm505251.htm

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

10. *June 6, KARE 11 Minneapolis* – (Minnesota) **141 Allina patients possibly exposed to TB.** Allina Health announced June 3 that it notified 141 patients who may have been exposed to tuberculosis (TB) by two workers, who had active TB, at Abbott Northwestern Hospital or Mercy Hospital in Minneapolis. The health care system advised the patients to schedule a free blood test at one of its clinics or seek medical attention if they experience any symptoms of TB.
Source: http://www.kare11.com/news/health/141-allina-patients-possibly-exposed-to-tb/234445183

Government Facilities Sector

11. *June 7, Portland Oregonian* – (Oregon) **20,000-acre wildfire burning in Malheur County: 'fire season starts when it decides to.'** Crews reached 50 percent containment June 7 of the 20,000-acre Owyhee Canyon Fire burning in Malheur County.
Source: http://www.oregonlive.com/pacific-northwest-news/index.ssf/2016/06/23000-acre_fire_burning_in_mal.html

12. *June 6, St. Louis Post-Dispatch* – (Missouri) **Former University of Missouri employee admits embezzling more than $700,000.** A former University of Missouri-Columbia administrative officer pleaded guilty June 6 in connection with a theft of over $716,000 from the school over the course of 9 years. The former employee created and registered three shell companies with the Missouri Secretary of State's Office, which were used to fraudulently bill the university for services that were never provided from January 2005 – June 2014.
Source: http://www.stltoday.com/news/local/education/former-university-of-missouri-employee-admits-embezzling-more-than/article_798dad22-befd-5582-9f54-b82ff63908a2.html

Emergency Services Sector

Nothing to report

Information Technology Sector

13. *June 7, SecurityWeek* – (International) **Facebook patches vulnerability in Messenger app.** Security researchers from Check Point discovered that the Facebook Messenger app was plagued with a vulnerability that could allow attackers to change the content of a conversation or replace legitimate links and files with malicious content. Attackers could exploit the flaw by obtaining identification (ID) assigned to each message via a request to "facebook.com/ajax/mercury/thread_info.php" and send another message with a duplicate ID to the victim.
Source: http://www.securityweek.com/facebook-patches-vulnerability-messenger-app

14. *June 7, IDG News Service* – (International) **Massive DDoS attacks reach record levels as botnets make them cheaper to launch.** Akamai released a report titled State of the Internet which revealed that during the first quarter of 2016, there were 19 distributed denial-of-service (DDoS) attacks that exceeded 100 Gigabits per second, making DDoS attacks four times more prevalent than the previous quarter. The report indicated that criminals could now afford to launch crippling attacks towards major companies.
Source: http://www.networkworld.com/article/3079987/massive-ddos-attacks-reach-record-levels-as-botnets-make-them-cheaper-to-launch.html#tk.rss_all

15. *June 6, Softpedia* – (International) **Angler exploit kit finds a method to escape Microsoft's EMET security toolkit.** Security researchers from FireEye reported that the Angler exploit kit (EK) installations were capable of bypassing Microsoft's Enhanced Mitigation Experience Toolkit (EMET) on Windows 7 to infect a system by deploying two exploits, one for Flash and one for Silverlight. The two exploits run their code via protected memory slots that allow them to deliver a malicious payload regardless of EMET's Data Execution Mitigation (DEP), Export Address Table Access Filtering (EAF), and EAF+ mitigations.
Source: http://news.softpedia.com/news/angler-exploit-kit-finds-a-method-to-escape-microsoft-s-emet-security-toolkit-504929.shtml

16. *June 6, Softpedia* – (International) **Black Shades ransomware asks victims only for a measly $30.** Several security researchers from various companies discovered a ransomware dubbed Black Shades Crypter was locking user files and demanding ransom money after finding that the ransomware adds an extra extension, ".silent" to encrypted files, informs victims to pay a small ransom to unlock their files, and encodes strings in its source code to make it difficult for malware analysts to decode.
Source: http://news.softpedia.com/news/black-shades-ransomware-asks-victims-only-for-a-measly-30-504935.shtml

17. *June 6, Softpedia* – (International) **Windows BITS Service used to reinfect computers with malware.** Security researchers from SecureWorks stated that attackers were using Window's Background Intelligent Transfer Service (BITS) to set up recurring malware download tasks, and then leveraging its autorun capabilities to install the malware after an investigation revealed that the original malware, called Zlob.Q, added malicious entries to the BITS service, which would download malicious

code on the system, run the malware, and erase itself when the infection is completed.
Source: http://news.softpedia.com/news/windows-bits-service-used-to-reinfect-computers-with-malware-504930.shtml

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

18. *June 7, WTOP 103.5 FM Washington, D.C.* – (Virginia) **Man dies in Fairfax apartment fire.** The City of Fairfax Fire Department is investigating a June 7 fire at a Fairfax apartment complex after the fire displaced 21 residents and killed 1 man.
Source: http://wtop.com/fairfax-county/2016/06/man-dies-fairfax-apartment-fire/

Dams Sector

19. *June 6, Kent Reporter* – (Washington) **Portion of Green River Trail in Kent to close for levee repairs.** Crews began repairing damaged and failing pavement on the Briscoe Levee June 6, prompting a 4 to 5 week closure of the Green River Trail in north Kent, Washington.
Source: http://www.kentreporter.com/news/381995471.html

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