

UNCLASSIFIED



NORTH DAKOTA

Critical Infrastructure and Key Resources (CI/KR) Ticker



The North Dakota Open Source (CI/KR) Ticker a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the (CI/KR) Ticker to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC DISCLAIMER

The (CI/KR) Ticker is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

TABLE OF CONTENTS

[North Dakota](#) 3

[Regional](#) 3

[National](#) 3

[International](#) 3

[Banking and Finance Industry](#) 4

[Chemical and Hazardous Materials Sector](#) 4

[Commercial Facilities](#) 5

[Communications Sector](#) 5

[Critical Manufacturing](#) 5

[Defense/ Industry Base Sector](#) 6

[Emergency Services](#) 6

[Energy](#) 7

[Food and Agriculture](#) 7

[Government Sector \(including Schools and Universities\)](#) 8

[Information Technology and Telecommunications](#) 9

[Public Health](#) 10

[Transportation](#) 11

[Water and Dams](#) 11

[North Dakota Homeland Security Contacts](#) 12

NORTH DAKOTA

(National) U.S. Army Corps of Engineers approves Dakota Access river crossing permits. The U.S. Army Corps of Engineers approved 200 water crossings and 3 Section 408 easements July 26, allowing the \$3.8 billion, 1,168-mile Dakota Access pipeline to cross U.S. Army Corps of Engineers property along its route from the Bakken region of North Dakota through Iowa and into Illinois. Energy Transfer Partners, the pipeline's developer, still requires approval for an easement in Illinois and an easement in South Dakota.

<http://www.thedickinsonpress.com/energy/bakken/4082041-us-army-corpsengineers-approves-dakota-access-river-crossing-permits>

REGIONAL

(Minnesota) BNSF train derails near Bena. Crews continued working July 25 to clear the wreckage from a July 22 BNSF train derailment near Bena, Minnesota, where 10 cars carrying coal derailed. Train service resumed July 25 following repairs to the tracks. <http://www.bemidjipioneer.com/news/local/4080798-bnsf-train-derails-nearbena>

NATIONAL

(National) Presidential Policy Directive – United States Cyber Incident Coordination. The U.S. President's administration released Presidential Policy Directive/PPD-41 July 26 detailing the U.S. Cyber Incident Coordination, which sets forth principles that govern the Federal Government's response to cyber incidents and the designation of responsibility to certain Federal agencies, including the FBI and DHS. <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policydirective-united-states-cyber-incident>

INTERNATIONAL

UNCLASSIFIED

(International) Patchwork cyber-espionage group evolves to target enterprises.

Researchers from Cymmetria and Symantec reported that the Patchwork advanced persistent threat (APT), also known as Dropping Elephant, cyberespionage group has begun targeting aviation, energy, financial, pharmaceutical, and software companies, among others, with malicious Microsoft PowerPoint and Word files in order to install Enfourks and Steladok backdoor trojans to obtain sensitive information from infected computers.

<http://news.softpedia.com/news/patchwork-cyber-espionage-group-evolves-to-target-enterprises-506623.shtml>

BANKING AND FINANCE INDUSTRY

(International) PayPal abused in banking trojan distribution campaign.

Proofpoint security researchers discovered malicious actors were distributing the Chthonic banking trojan, a variant of the Zeus malware, via legitimate looking PayPal emails to request money from users by sending money request messages claiming an illicit \$100 transfer was made to the victim's account which could be returned by clicking the malicious Goo.gl link that redirects the user to "katyaflash[.]com/pp.php," where the malware is downloaded onto the device in the form of an obfuscated JavaScript file that connects to the command and control (C&C) server. Researchers discovered the malware was also downloading a previously undocumented second-stage payload dubbed AZORult.

<http://www.securityweek.com/paypal-abused-banking-trojan-distributioncampaign>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

(Iowa) Authorities say chemical that rained down was fungicide. Officials are investigating a white fungicide that rained down on vehicles and houses in Marion, Iowa, July 26. Public health officials reported that hard surfaces should be thoroughly cleaned and that after 12 hours vegetation exposed to the fungicide will no longer pose a risk. http://qctimes.com/news/state-and-regional/iowa/authorities-say-chemical-that-rained-down-was-fungicide/article_a5ab9188-2817-5e39-8820-cbd9d3d05fbf.ht

UNCLASSIFIED

COMMERCIAL FACILITIES

(Florida) Fort Myers club shooting: 2 dead, more than dozen wounded after teen event. Two people were killed and at least 16 were hospitalized July 25 following a shooting at Club Blu Bar and Grill in Fort Myers, Florida. Officials detained three suspects in connection with the shooting and are investigating two other related shootings near the night club. <http://www.nbcnews.com/news/us-news/fort-myers-nightclub-shooting-1dead-14-others-reportedly-wounded-n615961>

COMMUNICATIONS SECTOR

(National) Defendants charged with participating in sophisticated international cell phone fraud scheme. The U.S. Department of Justice announced July 22 that three Florida residents were charged for their participation in a global cell phone fraud scheme where the defendants and coconspirators stole access to and fraudulently opened new cell phone accounts using the personal information of individuals around the U.S., in order to transmit thousands of international calls to Cuba, Jamaica, the Dominican Republic, and other countries with high calling rates. The conspirators also used reprogrammed cell phones and additional telecommunications equipment to run illegal call-termination businesses. <https://www.justice.gov/opa/pr/defendants-charged-participating-sophisticatedinternational-cell-phone-fraud-scheme>

CRITICAL MANUFACTURING

(International) 2015 Chrysler 200, Jeep Renegade; 2014 – 2015 Jeep Cherokee recalled: 410,000 vehicles affected. Fiat Chrysler Automobiles issued a recall July 26 for 323,000 of its model years 2014 – 2015 vehicles in select makes sold in the U.S. due to faulty wiring and software that could cause the vehicles to lose propulsion or stall. No injuries have been reported in connection with the recall which affects an additional 35,500 vehicles in Canada and 51,000 elsewhere.

UNCLASSIFIED

http://www.thecarconnection.com/news/1105198_2015-chrysler-200-jeeprenegade-2014-2015-jeep-cherokee-recalled-410000-vehicles-affected

(International) **Osram's intelligent home lighting system is riddled with flaws.** A researcher from Rapid7 discovered nine vulnerabilities affecting the Home and Pro versions of Osram's Lightify intelligent home lighting system running on Apple iOS7 or above and Android 4.1 or above that could allow attackers to discover the Wi-Fi Protected Access (WPA) pre-shared key of the user's home Wi-Fi and the network's password, to launch browser-based attacks against the user's workstation, control the light installations, and access confidential data. The vendor addressed nearly all problems in its latest patch set, with the exception of Secure Sockets Layer (SSL) pinning and issues related to ZigBee rekeying.

<https://www.helpnetsecurity.com/2016/07/27/osram-lightify-flaws/>

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

(Maryland) **Coast Guard seeks hoax caller whose 'maydays' cost \$500,000.** The U.S. Coast Guard announced July 22 that it is searching for a caller who has made 28 hoax distress calls originating around the Annapolis, Maryland area since July 2014. The calls have cost the service about \$500,000.

<http://wtop.com/maryland/2016/07/coast-guard-seeks-hoax-caller-whosemaydays-cost-500000-2/>

(National) **DOJ Report Finds One-Third Of Officers Killed Responding To Calls Were Alone.** The Washington Post reports that "although police officials have long recognized the need for two officers to respond on any kind of call with a potential for danger, a new study found that 34 percent of officers killed while responding to calls over a recent five-year period did not have backup when they were slain," and that "in many of the cases, they were dispatched alone, and sometimes they simply did not wait for a second officer to arrive."

UNCLASSIFIED

UNCLASSIFIED

<https://www.washingtonpost.com/news/true-crime/wp/2016/08/01/one-third-of-officers-killed-in-line-of-duty-were-alone-new-study-of-police-deaths-finds/>

(Arizona) Removal Of Arizona City's Speed Camera Leads To 178% Increase In Incidents.

The Arizona Republic (8/1, Boehm) reports the removal of a speed camera from an intersection in El Mirage, Arizona due a state law outlawing the devices has lead to a 178% increase in speeding incidents "over the last year, and collisions in the area [have] tripled."

<http://www.azcentral.com/story/news/local/surprise/2016/08/01/cameras-gone-grand-avenue-el-mirage-speeding-increases/86880718/>

ENERGY

(California) ENERGY: Statewide flex alert extended by 1 day. The California Independent System Operator issued a Flex Alert July 27 – July 28, asking residents to cut down and conserve energy during peak hours due to high temperatures in the State which puts the State's power grid under stress.

<http://www.pe.com/articles/stress-809205-landed-surrounding.html>

FOOD AND AGRICULTURE

(National) More sick; General Mills recalls 15 million more pounds of flour.

General Mills, Inc., expanded a previous recall July 25 to include an additional 15 million pounds of its Gold Medal flour, Signature Kitchens flour, and Wondra flour products after Federal health officials notified the company of 4 more confirmed cases of E.coli infections linked to the consumption of the flour products. Health officials reported the E.coli outbreak has sickened 46 people across 21 States since December 2015. http://www.foodsafetynews.com/2016/07/more-sick-general-mills-recallsmore-flour-traced-to-outbreak/#.V5dk_fkrKUK

(Nebraska) OSHA cites grain handling, processor for exposing workers to grain, noise, fall hazards at Nebraska site. The Occupational Safety and Health Administration cited New Alliance with 16 serious and 1 other-than-serious safety and health violations July 22 after February and March 2016 inspections at the Bridgeport, Nebraska facility revealed that the company exposed workers to fall

UNCLASSIFIED

UNCLASSIFIED

hazards and grain dust explosion hazards, failed to power down or lock out equipment to prevent unintentional operation, and failed to provide employees with equipment and training for grain rescue operations, among other violations. Proposed penalties total \$61,600.

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=32838

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(California) State of emergency declared to help battle Sand Fire. The acting governor of California declared a state of emergency July 26 for Los Angeles and Monterey counties due to the 37,701-acre Sand Fire and the more than 20,000-acre Soberanes Fire, which have prompted mandatory evacuations and the response of more than 3,000 firefighters. <http://abc7.com/news/state-of-emergency-declared-for-sand-fire/1443294/>

(Idaho) Fire managers warn drones could shut down flights near Idaho City. Crews worked July 28 to contain the 12,986-acre Pioneer Fire burning in the Boise National Forest in Idaho. The fire prompted the closure of Highway 21 from mile marker 48 to mile marker 72.5, and threatens at least 10 structures. <http://www.idahostatesman.com/news/local/environment/fires/article92120957.html>

(North Carolina) Former headmaster pleads guilty to wire fraud, faces up to 9 years in prison. The former headmaster of Southlake Christian Academy in North Carolina pleaded guilty July 28 to embezzling nearly \$9 million from the parochial school and its affiliated church, and using the funds for personal expenses and the personal expenses of an unnamed co-conspirator. The former headmaster attempted to hide the theft by opening 29 checking accounts, obtaining 26 credit cards, 7 loans, and creating 9 limited liability companies. <http://www.fox46charlotte.com/news/local-news/182783644-story>

UNCLASSIFIED

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

(International) Low-cost wireless keyboards open to keystroke sniffing and injection attacks. Bastille Networks researchers reported that a set of security flaws exploited via KeySniffer in low-cost wireless keyboards that are produced by at least 8 different vendors, can be exploited to collect passwords, security questions, and other sensitive financial and personal information due to a lack of encryption on keystroke data before it is transmitted wirelessly to the Universal Serial Bus (USB) dongle. Researchers noted that Bluetooth keyboards, wired keyboards, and higher-end wireless keyboards are not susceptible to KeySniffer. <https://www.helpnetsecurity.com/2016/07/26/keystroke-sniffing-wirelesskeyboards/>

(International) DDoS attacks increase 83%, Russia top victim. Nexusguard released a report showing that distributed denial-of-service (DDoS) attacks increased 83 percent to more than 182,900 attacks in the second quarter of 2016, with Russia as the top victim country. The U.S. and China were part of the top three targeted countries as the company also reported increases in routing information protocol (RIP) and multicast domain name service (mDNS) threats. <https://www.helpnetsecurity.com/2016/07/27/ddos-attacks-increase-russia-topvictim/>

(International) Siemens patches flaws in industrial automation products. Siemens released software updates addressing several vulnerabilities found in SIMATIC and SINEMA products including a cross-site scripting (XSS) vulnerability in the integrated Web server of SINEMA Remote Connect Server which can be exploited by a remote attacker by tricking the user into clicking on a specially crafted link, as well as two high severity improper input validation bugs that were discovered in SIMATIC WinCC SCADA systems and PCS7 distributed control systems (DCS), among other vulnerabilities. <http://www.securityweek.com/siemens-patches-flaws-industrial-automationproducts>

(International) Many web attacks come from United States: Sucuri. Researchers at Sucuri analyzed metadata from 30 days of Web traffic and blocked requests from its firewall product and found that the Structured Query Language (SQL) injection, brute force, and other exploit attempts had various browser user

UNCLASSIFIED

agents, more than one-third of the attacks came from the U.S. followed by Indonesia and China, and that when it came to operating systems (OS) 45 percent of attacks came from Microsoft Windows. <http://www.securityweek.com/many-web-attacks-come-united-states-sucuri>

(New York) New York Sex Offenders Barred From Playing Pokemon Go. Us Weekly reports sex offenders in New York will be barred from downloading or playing Pokémon Go according to new rules from the state Department of Corrections and Community Supervision. New York Governor Andrew Cuomo, who announced the directive, says the ban “will provide safeguards for the players of these augmented reality games and help take one more tool away from those seeking to do harm to our children.”

<http://mailview.bulletinmedia.com/mailview.aspx?m=2016080201leiu&r=8028317-3ed4&l=009-6c3&t=c>

PUBLIC HEALTH

(National) FDA updates warnings for fluoroquinolone antibiotics. The U.S. Food and Drug Administration approved safety label changes for fluoroquinolones, a class of antibiotics, July 26 to enhance warnings about the medication’s association with disabling and potentially permanent side effects, and recommended that prescribers limit use in patients with less serious bacterial infections. The labeling changes include an updated Boxed Warning and revisions to the Warnings and Precautions section of the label.

<http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm513183.htm>

(National) FDA approves Adlyxin to treat type 2 diabetes. The U.S. Food and Drug Administration approved Adlyxin, a once-daily injection to improve blood sugar levels in adults with type 2 diabetes July 28.

<http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm513602.htm>

UNCLASSIFIED

TRANSPORTATION

(National) Southwest Airlines still dealing with delays after outage. Southwest Airlines Co., reported July 23 that passengers continued to face flight cancellations and delays while the airline worked to resume normal operations after a computer router failure caused several technology systems to break down July 20, prompting the cancellation of at least 1,500 flights and the delay of 4,500 others.

http://www.sentinelenterprise.com/business/ci_30159978/southwestairlines-still-dealing-delays-after-outage

WATER AND DAMS

Nothing Significant to Report

UNCLASSIFIED

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center:** 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 **State Radio:** 800-472-2121; **Bureau of Criminal Investigation (BCI):** 701-328-5500; **North Dakota Highway Patrol:** 701-328-2455; **US Attorney's Office Intel Analyst:** 701-297-7400; **Bismarck FBI:** 701-223-4875; **Fargo FBI:** 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165

UNCLASSIFIED