

UNCLASSIFIED



NORTH DAKOTA HOMELAND SECURITY ANTI-TERRORISM SUMMARY



The North Dakota Open Source Anti-Terrorism Summary is 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 Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary 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.

QUICK LINKS

[North Dakota](#)

[Regional](#)

[National](#)

[International](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials
Sector](#)

[Commercial Facilities](#)

[Communications Sector](#)

[Critical Manufacturing](#)

[Defense Industrial Base Sector](#)

[Emergency Services](#)

[Energy](#)

[Food and Agriculture](#)

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

[Information Technology and
Telecommunications](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Public Health](#)

[Transportation](#)

[Water and Dams](#)

[North Dakota Homeland Security
Contacts](#)

UNCLASSIFIED

UNCLASSIFIED

NORTH DAKOTA

Man charged in hit-and-run at Grand Forks water treatment plant. A Grand Forks man was charged in a hit-and-run vehicle accident at the City of Grand Forks Water Treatment Plant after his truck ran over a small brick structure connected to a secure area of the water treatment building and fled the scene August 22. Source: <http://www.wdaz.com/event/article/id/19297/>

REGIONAL

(Minnesota) Enbridge Minn. pipeline plan needs more study, regulators say. Minnesota regulators determined that Enbridge Energy's pipeline expansion plans needed deeper study September 4 and sided with the Commerce Department when they determined the application did not provide enough documentation for the need of the expansion or its benefits. The company wants to install new pumps to an existing line that brings oil from sands in Alberta, Canada, across northern Minnesota to a refinery in Superior, Wisconsin. Source: <http://minnesota.publicradio.org/display/web/2013/09/04/environment/environmentalists-plan-enbridge-protest>

(Minnesota) NRC increases oversight of Monticello nuclear plant. The U.S. Nuclear Regulatory Commission (NRC) concluded that the Monticello nuclear power plant in Minnesota failed to maintain an adequate flood protection plan and cited it with a "yellow" violation of substantial safety significance. The NRC will increase inspections at the plant, and the plant's operator has taken actions to correct the issues. Source: <http://www.sctimes.com/article/20130829/NEWS01/308290076/NRC-increases-oversight-Monticello-nuclear-plant>

NATIONAL

Nothing Significant to Report

INTERNATIONAL

Syrian Electronic Army hacks Australian internet company, NYT and Twitter disrupted. Members of the Syrian Electronic Army hacktivist group caused disruptions and redirects on Web sites belonging to the New York Times, the Huffington Post, and Twitter August 27 after they breached Australian domain registration and hosting company Melbourne IT and modified the sites' DNS records. Source: <http://news.softpedia.com/news/Syrian-Electronic-Army-Hacks-Australian-Internet-Company-NYT-and-Twitter-Disrupted-378637.shtml>

BANKING AND FINANCE INDUSTRY

New, advanced banking trojan discovered in the wild. Researchers at ESET identified a new banking trojan with advanced features called Win32/Spy.Hesperbot targeting users in Turkey,

UNCLASSIFIED

UNCLASSIFIED

the U.K., and the Czech Republic via phishing emails. The trojan can log keystrokes, set up a remote proxy, create a hidden virtual network computing (VNC) server, and attempts to get users to install a mobile component of the malware on their mobile devices. Source: <http://www.darkreading.com/end-user/new-advanced-banking-trojan-discovered-i/240160826>

Citadel botnet resurges to storm Japanese PCs. Trend Micro reported that the Citadel botnet has returned to service and been spotted in a campaign targeting online banking credentials at Japanese financial institutions as well as email services such as Gmail, Yahoo Mail, and Hotmail. Source: http://www.theregister.co.uk/2013/09/04/citadel_wreaks_havoc_in_japan/

Osprey Packs hacked, customer credit card information stolen. Colorado-based Osprey Packs notified customers of its Pro Deal Web site that attackers might have used malware to obtain access to customers' credit card numbers and expiration dates, shipping and email addresses, names, and phone numbers. Source: <http://news.softpedia.com/news/Osprey-Packs-Hacked-Customer-Credit-Card-Information-Stolen-379584.shtml>

Fraud and identity theft camouflaged by DDoS attacks. Researchers at Prolexic detailed attack signatures associated with the Drive distributed denial of service (DDoS) toolkit, a tool often used in DDoS attacks that serve as a distraction while attackers attempt to compromise financial and e-commerce services. Source: <http://www.net-security.org/secworld.php?id=15492>

Cybercrime service automates creation of fake scanned IDs, other identity verification documents. Researchers at Group-IB identified a new Web-based cybercrime service that automates the creation of various forms of fake identification including passports, banking statements, and utility bills. Source: <http://www.networkworld.com/news/2013/082713-cybercrime-service-automates-creation-of-273262.html>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Nothing Significant to Report

COMMERCIAL FACILITIES

Refer to *Postal and Shipping* section, item #1 for related information

COMMUNICATIONS SECTOR

Eggheads turn Motorola feature phone into CITYWIDE GSM jammer. Research presenting at the 22nd USENIX Security Symposium showed how an attacker could take advantage of a vulnerability in the GSM communications protocol to deny service to a network or individual user by using a phone to masquerade as another handset and prevent the original from establishing an authenticated connection. Source:

UNCLASSIFIED

UNCLASSIFIED

http://www.theregister.co.uk/2013/08/28/german_boffins_mod_moto_into_citywide_gsm_jammmer/

CRITICAL MANUFACTURING

Toyota recalling 235,000 vehicles in U.S. Toyota announced two recalls totaling 235,000 vehicles in the U.S. The first recall affects Highlander Hybrid and Lexus RX 400h vehicles made between 2006 and 2010 due to a potential hybrid system overheating issue, while the second affects Lexus IS 350, IS 350C, and GS 350 vehicles produced between 2006 and 2011 due to a variable valve timing control issue. Source:

<http://www.11alive.com/news/article/305155/40/Toyota-recalling-235000-vehicles-in-US>

Ford recalls 370,000 sedans. Ford announced a recall of about 355,000 model year 2005-2011 Ford Crown Victoria, Mercury Grand Marquis, and Lincoln Town Car vehicles in the U.S. due to a corrosion problem that could lead to loss of steering. The recall includes about 195,000 Crown Victoria police models. Source: <http://wheels.blogs.nytimes.com/2013/08/31/ford-recalls-370000-sedans>

2011-2012 Chevrolet Cruze recalled for brake issue. General Motors announced a recall of 292,879 model year 2011 and 2012 Chevrolet Cruze compact sedans due to an issue where a supplemental braking pump may not activate, resulting in the reduction or loss of brake assist. Source: http://www.thecarconnection.com/news/1086541_2011-2012-chevrolet-cruze-recalled-for-brake-issue

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

FBI warns of “search for missing children” spear phishing emails. The FBI warned users of a spearphishing campaign using three malicious files in emails and documents purporting to be from its National Center for Missing and Exploited Children. Source:

<http://news.softpedia.com/news/FBI-Warns-of-Search-for-Missing-Children-Spear-Phishing-Emails-378537.shtml>

ENERGY

Hacker admits to selling access to U.S. Energy Department computers. A Pennsylvania man pleaded guilty to installing backdoors on several government, university, telecoms, and commercial systems and offering access to them in exchange for payment. Among others, the man offered undercover agents access to U.S. Department of Energy supercomputers that he had compromised via universities that had access to them. Source:

UNCLASSIFIED

UNCLASSIFIED

<http://news.softpedia.com/news/Hacker-Admits-Selling-Access-to-US-Energy-Department-Computers-378659.shtml>

FOOD AND AGRICULTURE

Chobani pulls yogurt cups, says no recall. Chobani reportedly asked various grocery retailers in the U.S. to pull its yogurt cups from shelves over quality concern issues stemming from customer reports of foul-smelling, sour yogurt which some customers have alleged sickened them. The company has not issued a formal recall and has not made clear which of its products are affected by the quality concerns. Source:

<http://www.foodsafetynews.com/2013/09/chobani-pulls-yogurt-cups-says-no-recall/>

Purina ONE beyOnd Dry Dog Food recalled for Salmonella risk. A limited number of 3 and one half pound bags of Purina ONE beyOnd Our White Meat Chicken & Whole Barley Recipe Adult Dry Dog Food was recalled by Nestle Purina PetCare Company because one bag of the product was found to be contaminated with Salmonella. Source:

<http://www.foodsafetynews.com/2013/09/purina-one-beyond-dry-dog-food-recalled-for-salmonella-risk/#.UiXwlpKko0c>

Goldenfeast recalls several brands of possibly tainted bird food. Several exotic bird foods have been recalled by Pennsylvania-based Goldenfeast, Inc. because of possible contamination by Salmonella virus from tainted parsley. Source:

http://www.upi.com/Top_News/US/2013/08/28/Goldenfeast-recalls-several-brands-of-possibly-tainted-bird-food/UPI-71681377716764/

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

Marine website compromised with pro-Syrian president message. No information was put at risk when a recruiting Web site for the Marine Corps was temporarily redirected to a message from the Syrian Electronic Army. Source: <http://news.msn.com/us/marine-website-compromised-with-pro-assad-message>

Man arrested for threats against Hawaii Rep. A man was arrested in Tijuana, Mexico, August 28 after he made alleged threats against a Hawaii representative. The suspect will be transported to Washington, D.C. after his initial court appearance. Source:

<http://www.lasvegassun.com/news/2013/aug/31/dc-gabbard-threats/>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

FTC: Negligence by security camera vendor harms customers' privacy. TRENDnet settled U.S. Federal Trade Commission charges that were brought due to lax security practices in software for its security cameras that allowed the cameras' feeds to be remotely posted and watched by

UNCLASSIFIED

UNCLASSIFIED

unauthorized users. Source: <http://www.networkworld.com/news/2013/090413-ftc-negligence-by-security-camera-273485.html>

Cybercriminals attach disassembled malware to malicious emails. Researchers at Symantec observed a targeted email attack technique that contains malware disassembled into several components that reassembles when a shortcut file is launched, helping the malware evade detection. Source: <http://news.softpedia.com/news/Cybercriminals-Attach-Disassembled-Malware-to-Malicious-Emails-379336.shtml>

Hackers targeting Java native layer vulnerabilities to insert malicious code. A Trend Micro researcher reported that cybercriminals are increasingly targeting native layer vulnerabilities in Java, showing increasing sophistication in attacks on Java. Source: <http://www.v3.co.uk/v3-uk/news/2291587/hackers-targeting-java-native-layer-vulnerabilities-to-insert-malicious-code>

Facebook scammers raking in \$200 MEEELLION in illicit profits. Two researchers who analyzed the pricing of Facebook spam used in various scams estimated that the spam trade brings in about \$200 million per year. Source: http://www.theregister.co.uk/2013/08/30/facebook_scammers_raking_in_200_meeellion_in_illicit_profits/

Cisco patches remote command execution flaw in Secure Access Control Server. Cisco issued a patch that closes a vulnerability in its Secure Access Control Server (ACS) that could be remotely exploited to execute arbitrary commands and take control of servers. Source: <http://news.softpedia.com/news/Cisco-Patches-Remote-Command-Execution-Flaw-in-Secure-Access-Control-Server-379326.shtml>

Researchers detail attacks for compromising Dropbox user accounts. Researchers presenting at the USENIX Security Symposium published a paper that details how to reverse engineer frozen Python applications, including the Dropbox client, as well as, how to intercept Dropbox server SSL traffic bypass the service's two factor authentication, and hijack Dropbox accounts. Source: <http://www.net-security.org/secworld.php?id=15480>

NATIONAL MONUMENTS AND ICONS

(California) Rim fire still 80% contained; pot farm as cause is debunked. California's Rim Fire grew to 237,341 acres September 4 as authorities lifted evacuation orders but kept several campgrounds and roads in Yosemite National Park closed. U.S. Forest Service investigators stated there was no evidence of any type of illegal marijuana growth in the area where the fire started, as previous news outlets reported. Source: <http://www.fresnobee.com/2013/09/04/3479714/rim-fire-still-80-contained-pot.html>

UNCLASSIFIED

UNCLASSIFIED

POSTAL AND SHIPPING

Pair charged with wire, mail fraud in buying scheme, allegedly hit stores in 20 states. Two men were charged with switching universal product codes on products at Home Depot stores, potentially defrauding the chain of \$1.3 million between November 2007 and August 2011. The men sold the products online for a profit and committed the crimes in at least 20 States.

Source: <http://www.therepublic.com/view/story/e8420aa20c0a4f6fb485d7585c362962/KY--Purchasing-Fraud-Charges>

PUBLIC HEALTH

13 patients possibly exposed to fatal brain disease. New Hampshire health officials announced September 4 that 8 brain-surgery patients at Catholic Medical Center in Concord may have been exposed to the rare, degenerative disorder, Creutzfeldt-Jakob Disease through potentially contaminated equipment. Five additional patients in other States may have also been exposed to the disease as a result of improperly sterilized surgical equipment. Source:

<http://www.usatoday.com/story/news/nation/2013/09/04/new-hampshire-hospital-fatal-brain-disease/2764645/>

TRANSPORTATION

Nothing Significant to Report

WATER AND DAMS

Nothing Significant to Report

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:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168

UNCLASSIFIED