

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

NORTH DAKOTA

Nothing Significant to Report

REGIONAL

Nothing Significant to Report

NATIONAL

Nothing Significant to Report

INTERNATIONAL

Nothing Significant to Report

BANKING AND FINANCE INDUSTRY

Credit reports sold for cheap in the underweb. Credit reports, Social Security numbers, and other personal information similar to that revealed in recent disclosures of celebrities' and political figures' information can be found for sale on several underground Web sites and forums. Source: <http://krebsonsecurity.com/2013/03/credit-reports-sold-for-cheap-in-the-underweb/>

J.P. Morgan Chase confirms denial-of-service attacks on Chase.com. J.P. Morgan Chase announced via Twitter that its Chase Online banking service was experiencing availability issues due to a denial of service (DoS) attack. Source: <http://www.foxbusiness.com/news/2013/03/12/jp-morgan-chase-confirmsdenial-service-attacks-on-chasecom/>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

NASA, DOE produce plutonium for first time in 25 years. The National Aeronautics and Space Administration and the U.S. Department of Energy have produced new plutonium-238 for use in spacecraft, the first new production of the fuel in 25 years. Source: <http://www.dailytech.com/NASA+DOE+Produce+Plutonium+for+First+Time+in+25+Years/article30127.htm>

COMMERCIAL FACILITIES

Nothing Significant to Report

UNCLASSIFIED

COMMUNICATIONS SECTOR

Google to pay \$7M for Wi-Fi eavesdropping. Google agreed to pay \$7 million to 37 States and the District of Columbia for its inadvertent collection of personal data during updates to its navigation service via Street View cars. The recorded data will be destroyed and the equipment and software used to collect will only be used with prior consent and notice. Source:

<http://www.csoonline.com/article/730152/google-to-pay-7m-to-states-for-wifi-eavesdropping>

CRITICAL MANUFACTURING

Nissan recalls 5 models for air bag problem. Nissan announced the recall of an undetermined number of model year 2013 Altima, Leaf, Pathfinder, Sentra, and Infiniti JX35 vehicles due to a faulty passenger airbag sensor. Source: <http://business.time.com/2013/03/13/nissan-recalls-5-models-for-air-bagproblem/>

Subaru recalls 47K vehicles that could start on their own. Subaru announced the recall of 47,419 Legacy and Outback vehicles from model years 2010-2013, Impreza vehicles from 2012, and XV Crosstek vehicles from 2013 due to their remote starters potentially starting the vehicle on their own. Source: <http://www.chicagotribune.com/business/breaking/chi-subaru-recalls-47k-vehicles-that-could-start-on-their-own-20130307,0,136713.story>

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

Nothing Significant to Report

ENERGY

(Louisiana) Copper thieves hit substations in Union Parish. Police are searching for criminals that stole over \$13,000 worth of copper wiring from a Claiborne Electric Co. substation tower in Marion. Source: <http://www.knoe.com/story/21582267/copper-thieves-hit-substations-in-unionparish>

FOOD AND AGRICULTURE

Utah dog food recalled because of salmonella contamination. Dog food products produced by Steve's Real Food of Murray were recalled due to potential salmonella contamination. Source: <http://www.foodsafetynews.com/2013/03/utah-dog-food-recalled-because-of-salmonella-contamination/#.UT3EtaU8zUg>

UNCLASSIFIED

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

OpBlackSummer: US Government sites CBP.gov and OPM.gov reportedly hacked. Members of two hacktivist groups have discovered SQL Interjection vulnerabilities on the Web sites of the U.S. Customs and Border Protection and the Office of Personnel Management that were validated by two researchers who were provided details of the vulnerabilities. Source: <http://news.softpedia.com/news/OpBlackSummer-US-Government-Sites-CPBgov-and-OPM-gov-Reportedly-Hacked-336836.shtml>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

It takes a company 243 days to discover a sophisticated attack, study shows. A report by Mandiant focusing on advanced persistent threats (APTs) outlined several findings, including that there are on average 243 days between an attacker gaining access and when the attack is uncovered. Source: <http://news.softpedia.com/news/It-Takes-a-Company-243-Days-to-Discover-a-Sophisticated-Attack-Study-Shows-337342.shtml>

China hackers keenest on industrial control system attacks – Trend Micro. A study by Trend Micro using false industrial control system (ICS) ‘honeypots’ collected information on ICS attack techniques, and noticed differences in attack types by country. Source: <http://www.techweekeurope.co.uk/news/china-hackers-industrial-systems-trend-110506>

Seagate blog compromised, leads to Blackhole and malware. Hard drive manufacturer Seagate’s blog has been compromised and altered to redirect visitors to sites hosting the Blackhole exploit kit. Source: http://www.net-security.org/malware_news.php?id=2440&

Treacherous backdoor found in TP-Link routers. Researchers have discovered a backdoor in some TP-Link routers that has the router download and execute a file when a specific URL is called. Source: <http://www.h-online.com/security/news/item/Treacherous-backdoor-found-in-TP-Link-routers-1822720.html>

NIST National Vulnerability Database down, malware identified on two Web servers. The National Institute of Standards and Technology (NIST) took down several of their Web sites, including the National Vulnerability Database (NVD) after malware was found on them. Source: <http://news.softpedia.com/news/NIST-National-Vulnerability-Database-Down-Malware-Identified-on-Two-Web-Servers-337103.shtml>

HP, CERT warn of critical hole in LaserJet printers. HP and DHS’s Computer Emergency Response Team (CERT) warned that some LaserJet printers manufactured by Hewlett-Packard (HP) have a security vulnerability that could allow remote data access to attackers. Source: http://threatpost.com/en_us/blogs/hp-cert-warn-critical-hole-laserjet-printers-031113

UNCLASSIFIED

Old and new botnets behind spam resurgence. Several botnets have been identified behind recent spam campaigns, with some being new botnets and others revamped older botnets.

Source: <http://www.net-security.org/secworld.php?id=14575>

NATIONAL MONUMENTS AND ICONS

Nothing Significant to Report

POSTAL AND SHIPPING

Medical provider data lost by N.C. gov't contractor. A contracted employee from the North Carolina Department of Health and Human Services lost a thumb drive that held the personal information from roughly 50,000 medical providers nationwide. The thumb drive was misplaced en route to a company facility and authorities will notify those affected.

Source: <http://hamptonroads.com/2013/03/medical-provider-data-lost-nc-govtcontractor>

PUBLIC HEALTH

Nothing Significant to Report

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