

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

Guilty pleas entered in ND mortgage fraud case. Two people charged in the case of a defunct Arizona mortgage lender accused of swindling Bismarck, North Dakota-based BNC National Bank out of about \$27 million pleaded guilty, the Associated Press reported December 1. The former director of accounting with American Mortgage Specialists Inc. (AMS) and an independent auditor were among four people charged in federal court. Two AMS executives pleaded guilty earlier to conspiracy to commit bank fraud and wire fraud. Authorities said AMS defrauded the bank by providing it with false financial statements and other information about the status of loans the bank had financed. Source:

http://www.wahpetondailynews.com/article_8019725a-3bca-11e2-b5bb-001a4bcf887a.html

REGIONAL

Nothing Significant to Report

NATIONAL

Nothing Significant to Report

INTERNATIONAL

Nothing Significant to Report

BANKING AND FINANCE INDUSTRY

‘Project Mayhem’ hacks accounting software. Researchers December 6 unleashed proof-of-concept code that would allow an attacker to basically write himself a check from the victim organization’s account. The Python-based tool is just one example of the type of advanced financial fraud that could be perpetrated against accounting applications and databases, according to SecureState researchers, who at Black Hat Abu Dhabi demonstrated their tool and findings on threats to accounting software. They focused their efforts on Microsoft’s Dynamics Great Plains application, but they said the same types of attacks could also be aimed at other accounting packages. No vulnerabilities were discovered or exploited in the Microsoft product. The Mayhem script detects that the Microsoft software is running, and creates a backdoor for the attacker to remotely make SQL queries and commit all types of financial fraud. —It doesn’t even need to install a traditional piece of [trojan] backdoor malware like most financial fraud malware does today, said the manager of SecureState’s penetration testing team. —We compare it with a banking trojan that hijacks [automated clearing house] ACH and wire transfers without the user’s knowledge, but this time we’re looking at the accounting system instead of the online banking session, he said. Microsoft’s accounting program is not the only potential victim. The manager said the same concept could be applied to MAS 90, Peachtree, Oracle, and SAP.

UNCLASSIFIED

Source:

<http://www.darkreading.com/databasesecurity/167901020/security/applicationsecurity/240144003/project-mayhem-hacksaccounting-software.html>

(Iowa) Officials: More than 90,000 Iowa residents affected by nationwide insurance data breach. Iowa officials said more than 90,000 residents in the State have been affected by a nationwide insurance breach that has impacted more than a million people, the Associated Press reported December 4. The breach affected customers for Nationwide Insurance and Allied Insurance. The Ohio based company posted news on its Web site about the October 3 intrusion, which explains personal data was compromised from both policy holders and non-policy holders. The company said it is not aware of any misuse of the information. The Iowa attorney general said Iowa residents may have been affected by the breach if they were seeking a competitive insurance quote through a company or third party agent that ran information through Nationwide.

Source:

<http://www.therepublic.com/view/story/ca836963edeb4ddda06405de389f6e52/IA--Data-BreachIowa>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Nothing Significant to Report

COMMERCIAL FACILITIES

Nothing Significant to Report

COMMUNICATIONS SECTOR

Nothing Significant to Report

CRITICAL MANUFACTURING

NHTSA recall notice - 2009-2012 BMW X5 engine belt idler pulley bolt. BMW announced December 6 the recall of 29,800 model year 2009-2012 X5 xDrive 35d SAV diesel vehicles manufactured from September 1, 2008 through November 15, 2012. The engine belt idler pulley bolt could loosen and break over time. If the engine belt idler pulley bolt breaks, the vehicle may unexpectedly lose power-assisted steering, increasing the risk of a crash. BMW will notify owners, and dealers will replace and tighten the idler pulley bolt. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcld_ID=12V55000&summary=true&prod_id=1454777&PrintVersion=YES

NHTSA recall notice - Ford Escape and Fusion fluid leak fire hazard. Ford is recalling 80,057 2013 Escape vehicles manufactured from October 5, 2011 through November 26, 2012 equipped with 1.6L engines; and 2013 Fusion vehicles manufactured from February 3, 2012

UNCLASSIFIED

UNCLASSIFIED

through November 29, 2012 equipped with 1.6L engines. The engines may overheat leading to fluid leaks that may come in contact with the hot exhaust system. Fluid leaks in the presence of an ignition source such as a hot exhaust system may result in a fire. The remedy for this recall campaign is still under development. Until the recall remedy has been performed, Ford is advising owners to contact their dealer or call the Ford telephone hotline to arrange alternate transportation. Source:

http://wwwodi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rclD=12V551000&summary=true&prod_id=1488829&PrintVersion=YES

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

Nothing Significant to Report

ENERGY

Nothing Significant to Report

FOOD AND AGRICULTURE

Nothing Significant to Report

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(South Carolina) School volunteer threatened to smuggle in gun, kill governor, police said. A woman was arrested and charged with making a threat against the South Carolina governor. Liberty police said the suspect was arrested December 4 and charged with threatening a public official. A district spokesman said the suspect — who was a volunteer with the Santa's Workshop program at the school — made the remark to a school employee December 4, when the governor was scheduled to speak. According to an incident report obtained by WSPA, the suspect said, "I'm going to smuggle a gun in and kill this Governor." Pickens County School District spokesman said she was a parent volunteer at Liberty Elementary, where the governor was scheduled to speak December 4. He said she made a remark to a staff member about harming the governor, and the school principal made the decision to call police. She said, "I felt like I had to take it seriously and report it to law enforcement. It's not up to me to decide whether there was any intent there or not, that's up to law enforcement to do so I turned it over to them." The suspect was arrested before the governor's arrival that day. Source:

<http://www2.wbtw.com/news/2012/dec/04/25/upstate-woman-arrested-aftermakingthreatagainst-ar-5100714/>

UNCLASSIFIED

UNCLASSIFIED

(South Carolina) SC inspector general: Centralize cyber security. South Carolina's inspector general recommended centralizing the cyber security functions of State agencies to help prevent another loss of personal data, according to a report released December 4. While oversight and standard-setting should be centralized, agencies should be allowed to tailor their policies according to their needs, he wrote. Inspector general said leaving the responsibility of data security to each agency leads to uneven data protection and prevents officials from managing or even understanding risks that could affect all State government. He noted the Division of State Information Technology can only suggest policies and lacks any authority to mandate statewide standards. The division offers federally funded security-monitoring services free to State agencies, local governments, and school districts. He recommended creating a new statewide chief security officer independent of the division, largely because of agencies' historical distrust of the division, which is part of the Budget and Control Board. He also believes the State should hire consultants to help transition to the centralized model. Source: <http://www.islandpacket.com/2012/12/04/2299978/sc-inspector-generalcentralize.html>

(Arizona) Man held after Social Security office blast. Authorities arrested a man during a traffic stop November 30 in connection with an explosion at the Social Security office in Casa Grande, Arizona, a law enforcement official said. The man was held under federal authority and faced possible State and federal charges, said an official with knowledge of the investigation. "He was heading eastbound on the main road out of the Casa Grande area," the official said. The explosion occurred early November 30 outside a door, causing a small fire and minimal damage, said Casa Grande fire marshal. No injuries were reported, an FBI spokeswoman said. The building was evacuated, but the surrounding buildings were not, according to the fire marshal. FBI bomb technicians, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and HAZMAT experts were participating in the investigation. Source: <http://www.koco.com/news/national/Man-held-after-Social-Security-office-blast/-/9844074/17614950/-/sepe5q/-/index.html>

(New York) State audit faults Fallsburg for lack of disaster plan for data security. The New York State Comptroller's Office recently found that the Town of Fallsburg needs to do a better job in securing computer data and assets. The comptroller evaluated computer security issues from January 1, 2011 through May 15. The comptroller recommended that the town assign user rights to its computers based on job descriptions. It also recommended moving its server to a secure area and formulating a plan that protects computer data during a disaster, including a secondary power source for the server. The supervisor wrote in the response letter that the comptroller has already assigned user rights based on job descriptions. He said that while the town will investigate back up systems, the server is backed up by a battery pack and tape. The supervisor wrote that it would be "cost prohibited" to move the server. The town could potentially build a locked cage around it. Source: <http://www.recordonline.com/apps/pbcs.dll/article?AID=/20121203/NEWS/121209935>

UNCLASSIFIED

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

80% of attacks are redirects from legitimate sites. Sophos released its Security Threat Report 2013, an assessment of what has happened in IT security for 2012 and what is expected for 2013. The increasing mobility of data in corporate environments has forced IT staff to become even more agile. 2012 was also a retro year driven by resurgence in traditional malware attacks, specifically malware distributed via the Web. For example, more than 80 percent of attacks were redirects, the majority of which were from legitimate Web sites that were hacked. While a large proportion of cybercrime continues to be opportunistic, Sophos believes that, in 2013, increased availability of malware testing platforms — some even providing criminals with money back guarantees — will make it more likely for malware to slip through traditional business security systems. The report also includes predictions concerning “irreversible” malware, attack toolkits with premium features, a decrease in vulnerability exploits, an increase in social engineering attacks, and attacks tied to the increasing integration of GPS and near field communication (NFC) functions. Source:

[http://www.netsecurity.org/secworld.php?id=14066&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+\(Help+Net+Security\)&utm_content=Google+Reader](http://www.netsecurity.org/secworld.php?id=14066&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader)

Hackers can use Twitter SMS vulnerability to post on users’ behalves, expert finds. A security researcher identified a vulnerability which can be leveraged by cybercriminals in attacks against Twitter users. According to the expert, an attacker only needs to know the mobile phone number associated with the target’s Twitter account. Presuming that the victim has enabled the SMS service and presuming that a PIN code is not set, the attacker can publish posts on their accounts by sending messages from a spoofed number. The researcher explains that many SMS gateways allow for the sender’s address to be set to an arbitrary identifier. Similar to email messages, an attacker can spoof the number to make it look like it comes from a specific number. The researcher claims that Facebook and Venmo were also affected, but they addressed the bug after he had reported the flaw to their security teams. Twitter responded December 4 stating that they fixed the vulnerability. A Romanian researcher that specializes in mobile security reveals that these types of vulnerabilities do not affect just social media platforms, but other services as well. “The problem is not only with Twitter, but also with other services (even banks) that authenticate the user based only on the phone number. It’s like just knowing someone’s username, no password needed, while in this case it’s even easier as people do not consider their phone number as something private.”

Source:

<http://news.softpedia.com/news/HackersCanUseTwitterSMSVulnerabilitytoPostonUsers-Behalves-Expert-Finds-311857.shtml>

Microsoft can retain control of Zeus botnet under federal court order. A federal court granted Microsoft permission to keep two major Zeus banking fraud botnets down for the next two years to allow more time to clean up trojan-infected computers. Microsoft won the court order November 28 to allow the company and its financial-services partners to continue to administer command-and-control servers for two Zeus botnets that had been shut down by the company’s

UNCLASSIFIED

legal and technical campaign in March. The motion for a default judgment, which was granted by the U.S. District Court in the Eastern District of New York, gives Microsoft and the National Automated Clearing House Association (NACHA) an injunction that allows the companies to keep the two Zeus botnets and their associated domains disabled for another 24 months. The original takedown, codenamed Operation b71, seized command-and-control servers in Pennsylvania and Illinois and disrupted the online-fraud networks. "This additional time will allow Microsoft to continue to work with Internet service providers and Computer Emergency Response Teams (CERTs) to clean those computers that are still infected with the malware," the senior attorney for Microsoft's Digital Crimes Unit said in an email interview. Source:

[http://www.eweek.com/security/microsoft-can-retain-control-of-zeus-botnet-under-federal-court-order/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+RSS/eweeksecurity+\(eWEEK+Security\)&utm_content=Google+Reader](http://www.eweek.com/security/microsoft-can-retain-control-of-zeus-botnet-under-federal-court-order/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+RSS/eweeksecurity+(eWEEK+Security)&utm_content=Google+Reader)

Season's gr3371ng5 - hacker releases exploits for MySQL and SSH. The hacker who goes by the name KingCope released several exploits December 2, some of which date back to 2011. The exploits mostly target the now-Oracle-owned MySQL open source database, but the SSH servers by SSH Communications Security and FreeSSHd/FreeFTPD are also at acute risk. The MySQL exploits do, however, require a legitimate database connection to execute injected code. Exploits such as "mysqljackpot" then, for example, misuse the connection's "file privilege" to provide the attacker with shell access at system privilege level. The hacker also describes a hole that allows attackers to trigger a database crash and another hole that enables them to find valid user names. Apparently, both holes can be exploited to bypass the password check and log in with an arbitrary password. With SSH's Tectia server, the exploit description says that attackers can modify a legitimate user's password by calling `input_userauth_passwd_changereq()` before logging in. In case of the FreeSSHd/FreeFTPD server, all that appears to be required is to ignore a refusal message by the server and declare the session to be open at the right time. All the exploit has to do is add an extra call to the existing `ssh_session2()` function of the regular openssh client. Source: <http://www.h-online.com/security/news/item/Season-s-gr3371ng5-hacker-releases-exploits-for-MySQL-and-SSH-1761125.html>

NATIONAL MONUMENTS AND ICONS

Nothing Significant to Report

POSTAL AND SHIPPING

Nothing Significant to Report

PUBLIC HEALTH

US health security research not balanced enough to meet goals, study suggests. Federal support for health security research is heavily weighted toward preparing for bioterrorism and

UNCLASSIFIED

UNCLASSIFIED

other biological threats, providing significantly less funding for challenges such as monster storms or attacks with conventional bombs, according to a new RAND Corporation study. The findings, published in the December issue of the journal Health Affairs, come from the first-ever inventory of national health security-related research funded by civilian agencies of the federal government. Researchers say recent events such as Superstorm Sandy, tornadoes in the Midwest, and major earthquakes around the world highlight the need to prepare the nation's health care system for a broad array of natural and manmade disasters. Beginning in 2010, researchers canvassed seven non-defense agencies whose research addresses topics relevant to the objectives of the National Health Security Strategy, a plan completed in 2009 to guide efforts by the government and others to defend the nation from a large-scale public health threats, both natural and manmade. More than 1,000 of the studies (66 percent) were directed toward biological threats, including bioterrorism, emerging infectious diseases, foodborne illness, and pandemic influenza. Fewer than 10 percent of the total pool of projects addressed natural disasters such as earthquakes, hurricanes, tornadoes, or floods. The remaining projects addressed threats that were chemical (8 percent), radiological (5 percent), nuclear (4 percent), or explosive (4 percent).

Source: http://www.eurekalert.org/pub_releases/2012-12/rc-uhs113012.php

Health care fraud investigations to net \$6.9B. The U.S. Office of Inspector General (OIG), which investigates health care fraud, expects to recover about \$6.9 billion from audits and investigations this year, the Cincinnati Business Courier reported December 4. Targets of investigations included hospitals, nursing homes, and the pharmaceutical industry. OIG reported 778 criminal actions against individuals or entities that engaged in crimes against Department of Health and Human Services programs, along with 367 civil actions. It also excluded 3,131 individuals and entities from participation in federal health care programs.

Source:

<http://www.bizjournals.com/cincinnati/blog/2012/12/healthcarefraudinvestigations.html>

CDC says Salmonella outbreak linked to Sunland peanut butter appears over. The Salmonella Bredeney outbreak that first appeared in September when several people were infected after eating a Trader Joe's Peanut Butter brand appears to be over, according to a Centers for Disease Control and Prevention (CDC) outbreak update November 30. The final number of cases in this outbreak stands at 42 cases in 20 States. There were no reported fatalities linked to this outbreak, although a quarter of the cases required hospitalization for their illness. The recalls of Sunland peanut products began September 22 with Trader Joe's voluntarily recalling its Creamy Salted Valencia Peanut Butter and removing the product from all store shelves. This was followed in quick succession by recalls of over 300 peanut-related products linked to the Portales, New Mexico company Sunland, Inc. Health officials said that although the outbreak appears over, many of these products have a long shelf-life, and they may still be in peoples' homes. Consumers unaware of the recall could continue to eat these products and potentially get sick. After a month-long U.S. Food and Drug Administration (FDA) inspection of Sunland's Portales plant, federal authorities suspended Sunland Inc.'s food facility registration November 26 prohibiting Sunland, Inc. from introducing food into interstate or intrastate commerce. FDA

UNCLASSIFIED

UNCLASSIFIED

will reinstate Sunland, Inc.'s registration only when they determine that the company has implemented procedures to produce safe products. Source:

<http://www.examiner.com/article/cdcsayssalmonellaoutbreaklinkedtosunlandpeanutbutter-appears-over>

TRANSPORTATION

(Colorado) New NextGen technology improves safety and efficiency in western Colorado. The Department of Transportation's Federal Aviation Administration (FAA) and Colorado Department of Transportation (CDOT) December 3 announced the activation of new NextGen technology that will help pilots address inclement weather around Montrose Regional Airport in western Colorado. The technology, known as Wide Area Multilateration (WAM), improves safety and efficiency by allowing air traffic controllers to track aircraft in mountainous areas that are outside radar coverage." Safety is our highest priority, and this is an excellent example of State and federal governments working together to not only improve safety and efficiency, but also provide immediate economic benefits," said the U.S. Transportation Secretary. "The new technology will help local businesses that depend on private and commercial aviation." The WAM deployment around Montrose is part of the Colorado Surveillance Project, which is a partnership between the FAA and CDOT, which began providing radar-like service to the mountain communities of Craig, Hayden, Steamboat Springs, and Rifle in 2009. The FAA and State of Colorado expect to complete the project by deploying WAM around Durango, Gunnison, and Telluride in the summer of 2013. Source:

http://www.faa.gov/news/press_releases/news_story.cfm?newsId=14093&cid=FB173

Highway traffic monitoring system has exploitable electronic flaw, says CERT. Systems that can track automotive traffic on roadways, providing speed and highway traffic behavior patterns has a flaw that could allow a skilled hacker to break in, according to the U.S. Industrial Control System Computer Emergency Readiness Team (ICS-CERT). A November 30 advisory issued by ICS-CERT said a specific system used by some municipal governments around the country has an authentication vulnerability that could allow unauthorized access. The advisory said Post Oak Bluetooth traffic systems that use Anonymous Wireless Address Matching (AWAM) were affected. AWAM systems detect vehicles that have Bluetooth — enabled networking devices aboard, including cellular phones, mobile GPS systems, telephone headsets, and in-vehicle navigation and hands-free systems. Each of those devices contains a unique electronic address that the AWAM system's sensors can read as the device travels by on a roadway. An independent research group said ICS-CERT on November 30 identified an insufficient entropy vulnerability in authentication key generation in Post Oak's AWAM Bluetooth Reader Traffic System. By impersonating the device, an attacker could obtain the credentials of the systems administrative users and potentially perform a Man-in-the-Middle (MitM) attack, intercepting communications within the organization. ICSCERT said Post Oak has validated the vulnerability and produced an updated firmware version that mitigates the potential opening. ICS-CERT said Post Oak said its products are deployed in the transportation sector, mainly in the U.S. Source: http://www.gsnmagazine.com/node/27933?c=cyber_security

UNCLASSIFIED

UNCLASSIFIED

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