

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

(Minnesota) 200-acre wildfire scars entry into Minnesota city. Some 100 firefighters spent May 18 working their way through the woods with chainsaws, hoses, and axes after a dangerous fire threatened Ely, Minnesota, the Minneapolis Star Tribune May 19. Officials from the Minnesota Incident Command, which is running the firefighting effort, said the nearly 200-acre fire was well under control late May 18, though they remained concerned that the warm, windy weather could still carry a burning branch outside the perimeter. A stretch of Highway 1 remained closed and residents of seven homes were still out after being ordered to evacuate. Response to the incident included four water-scooping air tankers and helicopters. By midday May 18, the effort had been downsized to three helicopters and one air tanker. Source: <http://www.firehouse.com/news/10719056/200-acre-wildfire-scars-entry-into-minnestoa-city>

NATIONAL

Critical industries don't grasp IT risks, study shows. A study by cybersecurity researchers at Carnegie Mellon University in Pittsburgh found that top corporate executives too often are disengaged from management of cyber risks to their organizations and that operators of critical infrastructure tend to lag behind the more highly regulated financial services industry in overseeing cybersecurity and privacy protection. The report, "How Boards & Senior Executives are Managing Cyber Risks," found that despite some improvements during the 4 years since the researchers' first study, there still is a lack of understanding of the importance of IT risks in overall enterprise risk management. Source: <http://gcn.com/articles/2012/05/21/carnegie-mellon-critical-infrastructure-risks.aspx>

INTERNATIONAL

Fukushima radiation higher than first estimated. The radiation released in the first days of the Fukushima nuclear disaster in Japan was almost 2.5 times the amount first estimated by Japanese safety regulators, the operator of the crippled plant said in a report released May 24. Because radiation sensors closest to the plant were knocked out by the March 11, 2011 quake and the tsunami, the utility based its estimate on other monitoring posts and data collected by Japanese government agencies. Tokyo Electric Power estimated meltdowns at three Fukushima reactors released about 900,000 terabecquerels of radioactive substances into the air during March. The estimate was based on measurements suggesting the amount of Iodine-131 released by the nuclear accident was three times higher than previous estimates, the utility said in the report. Iodine-131 is a fast-decaying radioactive substance produced by fission that takes place inside a reactor. It has a half-life of 8 days. More than 99 percent of the radiation released by the accident came in the first 3 weeks, the utility added. Source: <http://www.reuters.com/article/2012/05/24/nuclear-japan-idUSL4E8GO6ID20120524>

UNCLASSIFIED

Earthquake hits cheese production in northern Italy. The earthquake that struck northern Italy will affect production and export of some of the area's most internationally famous items — Parmigiano Reggiano and Grana Padano cheeses, Reuters reported May 22. National farmers' group Coldiretti estimated damage to agriculture in the area, one of Italy's most fertile and productive zones, at more than \$250 million. Some of the worst damage was to the production of Parmigiano Reggiano, also called Parmesan cheese, and Grana Padano. Some 300,000 wheels of Parmigiano Reggiano and 100,000 of Grana Padano, each weighing about 88 pounds, were damaged when they fell off shelves in warehouses where they were undergoing the 2-year-long seasoning process. Coldiretti said some 10 percent of the production of Parmigiano Reggiano and 2 percent of Grana Padano was affected by the quake. Source:

<http://www.reuters.com/article/2012/05/22/italy-quake-food-idUSL5E8GM9XG20120522>

BANKING AND FINANCE INDUSTRY

Banking malware spies on victims by hijacking webcams, microphones, researchers say. A new variant of SpyEye malware allows cybercriminals to monitor potential bank fraud victims by hijacking their Web cams and microphones, according to security researchers from Kaspersky Lab May 21. SpyEye is a computer trojan that specifically targets online banking users. Like its older cousin, Zeus, SpyEye is no longer being developed by its original author but is still widely used by cybercriminals. SpyEye's plug-in-based architecture allows third-party malware developers to extend its original functionality, a Kaspersky Lab malware researcher said. This is exactly what happened with the new Web cam and microphone spying feature, implemented as a SpyEye plug-in called flashcamcontrol.dll, he said. As suggested by the DLL's name, the malware accesses the two computer peripherals by leveraging Flash Player, which has Web cam and microphone control functionality built in. Under normal circumstances, users get prompted to manually allow Web sites to control their computers' Web cam and microphone via Flash. However, the SpyEye plug-in silently whitelists a list of online banking Web sites by directly modifying Flash Player configuration files. Source:

http://www.computerworld.com/s/article/9227387/Banking_malware_spies_on_victims_by_hijacking_webcams_microphones_researchers_say

FDIC sues big banks over mortgage debt losses. The U.S. government filed three lawsuits against large banks over losses on soured mortgage debt purchased by two small Illinois banks that failed in 2009, Reuters reported May 21. Acting as receiver for Citizens National Bank and Strategic Capital Bank, the Federal Deposit Insurance Corp (FDIC) sued many banks including Bank of America Corp., Citigroup Inc., Deutsche Bank AG, and JPMorgan Chase & Co. Seeking a combined \$92 million, the lawsuits accuse the banks of misrepresenting the risks of residential mortgages they packaged into securities, causing losses for investors once the poor quality and defective underwriting became evident. Two FDIC lawsuits were filed in New York federal court and seek a combined \$77 million, while a third filed in Los Angeles seeks \$15 million. Bank of America and Citigroup were the only banks named as defendants in all three cases. Deutsche Bank and JPMorgan were defendants in two cases, and Ally Financial Inc., Credit Suisse Group AG, HSBC Holdings Plc., Royal Bank of Scotland Group Plc., and UBS AG in one. Citizens National

UNCLASSIFIED

UNCLASSIFIED

and Strategic Capital, based in Macomb and Champaign, Illinois, respectively, had roughly \$1 billion of combined assets when they were closed May 22, 2009. Source:

http://articles.chicagotribune.com/2012-05-21/business/sns-rt-us-fdic-bank-lawsuitsbre84k1b4-20120521_1_renee-calabro-fdic-lawsuit-royal-bank

Trojan stealing money in German online banking scam. Trusteer came across a complex new criminal scheme involving the Tatanga trojan that conducts an elaborate Man in the Browser (MitB) attack to bypass SMS based transaction authorization to commit online banking fraud. The scam targets online banking customers of several German banks. When the victim logs on to the online banking application, Tatanga uses a MitB webinject that alleges the bank is performing a security check on their computer and ability to receive a Transaction Authorization Number (TAN) on their mobile device. In the background, Tatanga initiates a fraudulent money transfer to a mule account. It even checks the victim's account balance and will transfer funds from the account with the highest balance if there is more than one to choose from. The victim is asked to enter the SMS-delivered TAN they receive from the bank into the fake Web form as a way to complete the security process. By entering the TAN in the injected HTML page, the victim is approving the fake transaction originated by Tatanga. Once the victim enters the TAN in the fake form and hits submit, the funds are transferred to the fraudster's account. Meanwhile, Tatanga modifies the account balance reports in the online banking application to hide the fake transaction. Source: http://www.net-security.org/malware_news.php?id=2118&utm

Fake Amex ID verification email leads to malware. A bogus American Express account ID verification e-mail is currently making the rounds, trying to trick users into following the offered links. The e-mail might look like a phishing one at first glance, but it is not. "Those who click the link will be taken to a webpage that advises them to wait while the page is loading," Hoax-Slayer said. "However, an American Express login page does not appear as the user would expect. Instead, the page will redirect to another site that harbors the BlackHole exploit kit." This spam run is the latest in a long line of similar ones targeting a wide variety of users, and for the victims, it usually ends up with information-stealing malware being installed on their computers. Source: http://www.net-security.org/malware_news.php?id=2115&utm

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

U.S. charges Chinese man with illegal nuclear-related exports. A Chinese national was charged with illegally exporting to China U.S.-made sensors used to produce weapons-grade uranium, the U.S. Department of Justice said May 23. The man, a sales manager for a Chinese subsidiary of MKS Instruments located in Andover, Massachusetts, was arrested at his hotel in North Andover, Massachusetts, and charged with conspiracy to violate U.S. export laws. He allegedly allowed thousands of pressure measuring sensors, known as pressure transducers, to be exported from the United States to unauthorized users in China, the department said. He was accused of co-conspiring with others since 2007 to export pressure transducers from the United States to unauthorized end-users by using export licenses issued to MKS customers and/or

UNCLASSIFIED

UNCLASSIFIED

through export licenses obtained in the name of a front company. Source:

<http://www.reuters.com/article/2012/05/23/usa-china-arrest-idUSL1E8GNIKX20120523>

COMMERCIAL FACILITIES

(Georgia) Police seek help from feds after 2 clinic fires. Federal authorities have been asked to help investigate after two fires in the past week at women's clinics in metro Atlanta. Authorities said the latest fire happened May 23 at a Marietta obstetrics and gynecology office that advertises itself as an "abortion services" clinic. A Cobb County fire spokeswoman said it took more than 20 firefighters to put out the flames. There were about 20 employees and several patients inside when the fire started. Gwinnett County fire officials said a fire May 20 at the Atlanta Gynecology and Obstetrics Gwinnett office in Lilburn is suspicious. A Gwinnett police official said the Bureau of Alcohol, Tobacco, Firearms and Explosives has been asked to help investigate. Some women's clinics have also been burglarized in recent months. Source:

<http://www.firstcoastnews.com/news/article/257532/5/Police-seek-help-from-feds-after-2-clinic-fires>

COMMUNICATIONS SECTOR

Smartphone hijacking vulnerability affects AT&T, 47 other carriers. Computer scientists identified a vulnerability in the network of AT&T and at least 47 other cellular carriers that allows attackers to surreptitiously hijack the Internet connections of smartphone users and inject malicious content into the traffic passing between them and trusted Web sites. The attack, which does not require an adversary to have any man-in-the-middle capability over the network, can be used to lace unencrypted Facebook and Twitter pages with code that causes victims to take unintended actions, such as post messages or follow new users. It can also be used to direct people to fake banking sites, and to inject fraudulent messages into chat sessions in some Windows Live Messenger apps. Source:

<http://arstechnica.com/security/2012/05/smartphone-hijacking-on-att-47-other-carriers/>

CRITICAL MANUFACTURING

Cooper Lighting recalls commercial reflector assembly with glass lens due to injury hazard.

The U.S. Consumer Product Safety Commission, in cooperation with Cooper Lighting, May 23 announced a voluntary recall of about 21,000 Portfolio 7-inch reflector assemblies with glass lenses. Consumers should stop using recalled products immediately unless otherwise instructed. The reflector can fall out of its fixture to the ground, which could result in an injury hazard. Cooper Lighting has received 23 reports of reflectors falling. The recall involves circular, 7-inch diameter Portfolio aluminum reflector with glass lens designed to be inserted into a light fixture. This reflector is intended for use in indoor, commercial applications, such as office buildings, schools, and shopping malls. Source:

<http://www.cpsc.gov/cpscpub/prerele/prhtml12/12185.html>

UNCLASSIFIED

UNCLASSIFIED

Fire risk brings recall of nearly 87,000 Jeeps. Chrysler is recalling nearly 87,000 Jeep Wranglers in the United States, Canada, and elsewhere due to a risk of fires, the Associated Press reported May 19. U.S. safety regulators said the recall affects only Wranglers from the 2010 model year with automatic transmissions. Debris can get caught between a transmission plate and the catalytic converter, causing a fire. At least 14 complaints of fires caused by the problem were reported. Source: <http://www.cbsatlanta.com/story/18564296/fire-risk-brings-recall-of-nearly-87000-jeeps>

DEFENSE/ INDUSTRY BASE SECTOR

DOD pledges action against suspect electronics. A planned U.S. Defense Department initiative would bolster efforts to prevent armed forces hardware from incorporating off-brand components from China, the Washington Times reported May 22. May 22, a Defense Department spokesman said the Pentagon is “working very hard to try to sort this issue out, and take steps to further strengthen our supply chain.” In a related move, the department finalized instructions in March aimed at laying the groundwork for a formal initiative to target illicit defense components. Bolstering transparency mandates for companies hired by the government is the goal of a collaborative effort by the White House and Pentagon, the spokesman added. Source: <http://www.nti.org/gsn/article/defense-department-pledges-action-against-fake-defense-electronics/>

China top source of counterfeit U.S. military electronics. China’s government has failed to curb manufacturing of counterfeit military electronic parts by Chinese companies that are the “dominant source” of fakes in the U.S. defense supply chain, a U.S. Senate investigation found. In January, the U.S. Air Force suspended a Shenzhen, China-based company from supplying parts to U.S. contractors after it sold about 84,000 suspect components, many of them installed on U.S. aircraft, according to an example cited in the U.S. Senate Armed Services Committee report released May 21. The panel’s report outlines the results of a 14-month investigation disclosing dozens of examples of suspected counterfeit electronic parts. Saying U.S. companies and the military services did not crack down on abuses, the committee said the defense industry “routinely failed to report cases of suspect counterfeit parts, putting the integrity of the supply chain at risk.” The report did not cite any examples of counterfeit parts causing damage such as lives lost or planes that crashed. The committee said it found “overwhelming and undeniable evidence to support” the conclusion that China has not taken steps to stop operations “that are carried out openly in that country.” Source: <http://www.bloomberg.com/news/2012-05-21/china-top-source-of-counterfeit-u-s-military-electronics.html>

EMERGENCY SERVICES

(Texas) More white powder scares. Crews: response costly. Another “white powder” scare occurred May 19 in Dallas at a synagogue. Two young men were seen walking through the parking lot of the synagogue before a morning service. A witness said they were deliberately placing a white, powdery substance in the parking lot and on the sidewalk. The incident was the

UNCLASSIFIED

UNCLASSIFIED

latest in a string of scares across North Texas. The substance was determined to be rice powder. Source: <http://www.myfoxdfw.com/story/18562453/more-white-powder-scares-response-costly?obref=obinsite>

ENERGY

(Texas) Copper thief strikes at Bowie Co. substation. Sheriff's deputies in Bowie County, Texas, investigated a copper theft at an electrical substation, KSLA 12 Shreveport reported May 23. Deputies said the theft happened at the Ridge Springs substation at the Bowie-Cass Electrical Cooperative Company near Texarkana. Company officials said the removal of the copper caused live wires to hit the metal frame of the substation melting the metal out of the cement May 23. Officials said the live wires left scorch marks on the ground and caused a strong, noticeable odor. Investigators said they initially believed the scorch marks and the odor was from remains of a body, but later determined no one died. Source: <http://www.ksla.com/story/18609339/copper-thief-strikes-at-bowie-co-substation>

(Kansas) Thieves steal copper from Westar Energy. Thieves broke into a Westar Energy warehouse in Wichita, Kansas, and took thousands of dollars worth of copper. The theft was discovered May 19 when Westar employees noticed someone cut a chain-link fence surrounding the property in several locations, according to a spokesman for the Wichita Police Department. Once inside the warehouse, the thieves used a skid loader to steal the copper. The loader was later found outside the property in an abandoned field. Source: <http://www.kansas.com/2012/05/20/2342206/thieves-steal-copper-from-westar.html>

(Utah) Utah utility customers targeted by scams offering bill credits. The Utah Department of Commerce and Rocky Mountain Power warned Utah utility customers to be aware of scammers posing as Rocky Mountain Power customer service agents or attorneys, KCSG 14 St. George reported May 21. During the con, elderly consumers are told that under a grant authorized by the U.S. President, they can receive a utility bill credit or have their bills paid directly. The potential victims are told they must provide their Social Security number, credit card, or check routing number first. The scam has been reported across the country and in Utah in recent months. Some scammers are handing out flyers in person, while others are using social media, texting, or contacting consumers by phone. Some customers who received such calls were told their electricity will be disconnected if they do not provide their credit card information. Source: http://www.kcsg.com/view/full_story/18671626/article-Utah-Utility-Customers-Targeted-By-Scams-Offering-Bill-Credits?instance=home_first_stories

FOOD AND AGRICULTURE

Wheat fields parched by drought from U.S. to Russia: Commodities. Droughts withering wheat crops from the United States to Russia to Australia will probably spur the biggest reduction in global supply estimates since 2003 and drive prices to the highest in almost a year, Bloomberg reported May 24. Kansas, the top U.S. grower of winter wheat, is poised for its driest May on record, the State's climatologist estimated. Ukraine and Russia, accounting for 11 percent of

UNCLASSIFIED

UNCLASSIFIED

world output, have endured drought conditions for 3 months, University College London data show. The U.S. Department of Agriculture may cut its global crop estimate by 1.2 percent in June, the biggest drop in a June report since 2003, according to the average of 18 analyst estimates compiled by Bloomberg. Winter wheat accounted for about 75 percent of U.S. output in 2011 and is the main variety grown in the Black Sea region. Source:

<http://www.bloomberg.com/news/2012-05-23/wheat-fields-parched-by-drought-from-u-s-to-russia-commodities.html>

(Maryland) Maryland first State to ban arsenic in poultry feed. Maryland's governor signed a bill May 22 banning arsenic in poultry feed, making his State the first to have a law against the practice on the books. The new law, which takes effect January 1, 2013, prohibits the use, sale, or distribution of commercial feed containing arsenic and specifically mentions two Pfizer drugs that contain arsenic: Roxarsone, which the company voluntarily withdrew from the market in 2011, and Histostat, which is still on the market. The move followed a U.S. Food and Drug Administration (FDA) study released the summer of 2011 that found increased levels of inorganic arsenic in the livers of chickens treated with Roxarsone. The new data raised concerns of a "very low but completely avoidable exposure to a carcinogen," said the FDA's deputy commissioner for foods, when FDA announced the company was withdrawing the drug in response to the study's findings. FDA said the arsenic levels found in their poultry study are low enough that consumers are not at risk eating poultry while Roxarsone is phased out of use in the United States. Source: <http://www.foodsafetynews.com/2012/05/maryland-first-state-to-ban-arsenic-in-poultry-feed/>

Salmonella Paratyphi B outbreak grows. The Salmonella Paratyphi B case-count associated with contaminated starter culture used in raw tempeh products sold by Smiling Hara, an Asheville, North Carolina-based company, continued to grow the week of May 17, with the number of Salmonella Paratyphi B cases reaching 83, May 18. According to the Asheville Citizen-Times, 62 of the cases were counted among residents of Bruncombe County, North Carolina. Smiling Hara purchased the contaminated spore culture from Tempeh Online, a Maryland-based company that has since taken down its Web page and deleted all but one of its Twitter posts. The U.S. Food and Drug Administration was working with State health officials to determine whether or not Tempeh Online's contaminated culture might have been used by any other producers. Smiling Hara recalled all of its tempeh made between January 11 and April 11 with best-by dates of July 11 through October 25. Source: <http://www.foodsafetynews.com/2012/05/salmonella-paratyphi-b-outbreak-grows/>

Diamond Pet Foods recalls more dry dog food. Diamond Pet Foods again recalled batches of dry dog food that may be contaminated with Salmonella, this time to include its Diamond Naturals Small Breed Adult Dog Lamb & Rice Formula dry dog food manufactured August 26, 2011, Food Safety News reported May 22. The earlier recalls involved various formulas manufactured after December 9, 2011 at Diamond's production facility in Gaston, South Carolina. This recall involves food produced in Meta, Missouri. The most recent recalled product was distributed in Colorado, Illinois, Kentucky, Louisiana, Michigan, Minnesota, Missouri, Oklahoma, Pennsylvania, South Dakota, Tennessee, Texas, and Wisconsin. Further

UNCLASSIFIED

UNCLASSIFIED

distribution through other pet food channels, including online retailers, may have occurred. For the earlier recalls, as of May 11, 15 people in 9 states and 1 person in Canada were reported sickened with an outbreak strain of Salmonella Infantis from contact with contaminated dog food or infected animals, said the Centers for Disease Control and Prevention. As of May 16, the Food and Drug Administration confirmed two dog illnesses related to the outbreak. The week of May 17, the Calgary Herald in Alberta reported two cats in a Montreal shelter died, and another was ill, after being fed Diamond products. Source:

<http://www.foodsafetynews.com/2012/05/diamond-pet-foods-recalls-more-dry-dog-food/>

USDA takes meat and poultry labeling to the web. A new Web-based label approval system that will streamline the agency's review process for meat, poultry, and egg product labels was introduced May 21 by USDA's Food Safety and Inspection Service (FSIS). Called the Label Submission Approval System (LSAS), the new system will: make it possible for food manufacturers to submit label applications electronically; flag application submission errors that could delay the approval process; and allow users to track the progress of their submission. The LSAS is supposed to reduce the time and costs incurred by the industry and the agency. Until the launch of LSAS, companies mailed or hand delivered paper applications to FSIS, and it reviewed and corrected them before returning them in hard copy. The agency receives 150 to 200 label submissions daily, and it can take more than 3 weeks for a label to be reviewed. The Web-based system will make approved or corrected labels immediately available to companies, saving time and mailing costs. The new system also will allow companies to store labels and make changes electronically, removing the need to print and re-submit modified labels for review to FSIS each time a change is made. Source:

<http://www.foodsafetynews.com/2012/05/usda-takes-meat-poultry-labeling-to-the-web/>

River Ranch expands salad recall because of possible health risk. River Ranch Fresh Foods, LLC of Salinas, California, is expanding its voluntary recall of retail and food service bagged salads because they have the potential of being contaminated with Listeria monocytogenes. Retail salad products under this recall were distributed throughout the United States and Canada under various sizes and packaged under the brand names of River Ranch, Farm Stand, Hy-Vee, Shurfresh, and The Farmer's Market. Food service salad products under this recall were distributed throughout the United States and Canada under various sizes and packaged under the brand names of River Ranch and Sysco. The recalled salad bags have either —Best By code dates between May 12-29 or Julian dates of 118 and 125. Source:

<http://www.fda.gov/Safety/Recalls/ucm304741.htm>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

Computer hackers access U.S. Justice Department website: Spokeswoman. One or more unauthorized users gained access to the inner workings of a Web site run by the U.S. Justice Department, a department spokeswoman said May 21 after the hacker group Anonymous said they were behind the incident. The hackers accessed a server that operates the Bureau of

UNCLASSIFIED

UNCLASSIFIED

Justice Statistics' Web site, the spokeswoman said. The department was looking into whether the unauthorized users broke criminal laws, she said. Online statements attributed to Anonymous said they were responsible for the security breach, and the files they obtained included e-mails. Source: <http://www.reuters.com/article/2012/05/21/net-us-usa-hackers-idUSBRE84K1B720120521>

(Connecticut) Students expelled over Internet posts. Two West Haven High School students accused of making threats on Twitter were charged and expelled from the Connecticut school, the Associated Press reported May 22. A police sergeant said teachers found the tweets in early May. The tweets, posted by a junior and a sophomore, did not appear to be linked to each other. The junior allegedly posted several messages about placing a bomb in a locker. The sophomore allegedly sent a tweet about shooting himself and other people. Police said the students' homes were searched and no weapons were found. Both students face felony charges. Source: <http://www.nbcconnecticut.com/news/local/Students-Expelled-over-Internet-Posts-152521765.html>

White powder case costs millions in first response. Federal authorities are tracking what they call the most prolific mailer of white powder in U.S. history with an eye toward solving a case that has tied up first responders and cost taxpayers millions of dollars, Associated Press reported May 17. Officials with the FBI and the U.S. Postal Inspection Service believe the same person has sent nearly 400 letters containing nontoxic white powder across the United States and abroad from Texas. Officials stressed that each incident diverts police, fire personnel, and other valuable resources from genuine emergencies, increasing the urgency of finding the perpetrator. Postal processing plants have biohazard detection systems that can find toxic substances, but first responders are typically called when letters with white powder are delivered — a result of the anthrax attacks in 2001. A spokesman for the Dallas Fire-Rescue Department said hazardous material teams of 10 to 16 respond to white powder calls. Each response, which can last about 2 hours, requires about \$1,500 per hour in fuel and other equipment-related costs on top of salaries, he said. Source: <http://abcnews.go.com/US/wireStory/white-powder-case-costing-millions-investigate-16370588#.T7Z0BVK1VvB>

NASA investigating possible SSL compromise. A NASA spokesperson told SecurityWeek they were investigating claims made by a group of Iranian hackers May 16 that they have compromised the SSL certificate used on the NASA Solicitation and Proposal Integrated Review and Evaluation System (NSPIRES) Web site. The Iranian student group comprised of programmers and hackers — known as the Cyber Warriors Team — said the certificate was compromised by exploiting an existing vulnerability within the portal's log-in system. Once they had control over the certificate, they claimed to have used it to —obtain User information for thousands of NASA researcher With Emails and Accounts of other users [sic]. Source: <http://www.securityweek.com/nasa-investigating-possible-ssl-compromise>

(Wisconsin) Man charged with threat to blow up Democratic Party headquarters. Federal authorities charged a Madison, Wisconsin man May 19 with making a telephone threat in

UNCLASSIFIED

UNCLASSIFIED

February to blow up the offices of the Democratic Party of Wisconsin, among more than 100 calls that he allegedly placed to the office this year. He repeatedly threatened to shoot Democrats on the streets around the Wisconsin capital and those supporting the recall of the governor in phone calls he made to the Democratic Party's office in January, February, and March, according to an FBI affidavit filed in U.S. district court in Madison. Source:

http://lacrossetribune.com/news/local/crime-and-courts/man-charged-with-threat-to-blow-up-democratic-party-headquarters/article_95985afe-a176-11e1-90d0-001a4bcf887a.html#ixzz1vVaDJNOq

(Maryland) NORAD intercepts 2 aircraft near Camp David. Military aircraft intercepted two small planes in restricted airspace around Camp David, Maryland, where world leaders gathered for an economic summit. The North American Aerospace Defense Command (NORAD) said the two Cessna 172 aircraft were out of radio communication May 18 inside a 30-mile restricted area around the U.S. Presidential retreat. The restricted area was expanded temporarily for the Group of Eight talks. A U.S. Secret Service spokesman said the violations were not deemed to be threatening. Source:

<http://www.google.com/hostednews/ap/article/ALeqM5h7h1z8nYLbbJaHj1sBv396CjRogA?docId=40ec25f1eaa48a1998fd639a5377cdb>

(Illinois) Chicago terror plot with Molotov cocktails foiled. Three men were accused of planning terrorist attacks during the May 20-21 North Atlantic Treaty Organization summit of world leaders in Chicago, the county prosecutor said. The three men "were charged overnight with criminal acts relating to terrorism, conspiracy to commit terrorism and possession of explosives," said the Cook County state's attorney in a statement May 19. The men were accused of making Molotov cocktails to hurl at the U.S. President's re-election campaign headquarters in Chicago, at the home of Chicago's mayor, and at financial institutions and police stations, according to a statement issued by the county prosecutor and Chicago's police superintendent. Source: <http://www.businessweek.com/news/2012-05-19/three-accused-of-chicago-terror-plot-before-nato-summit>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

McAfee reports big spike in malware. PC malware had its "busiest quarter in recent history," according to McAfee's quarterly security report released May 23. The security company registered the biggest increase in malware in 4 years during the first quarter of 2012, bringing the total number of samples to 83 million. Fake antivirus programs declined in popularity, but software with faked security signatures, rootkits, and password-stealing trojans rose. McAfee counted about 200,000 new examples of password-stealing trojans. Software is "signed" by the vendor to tell users it is safe to install. A user is more likely to trust Microsoft or McAfee, for example, than an unknown vendor. Scammers capitalize on that trust when they forge the digital signature of a trusted provider to boost the chances of having their malware successfully installed on the user's computer. Security researchers began to warn that forged security signatures would increase after the success of the proliferation of the Stuxnet and Duqu malware programs that used that deception. Among botnets, Cutwail was most active during

UNCLASSIFIED

UNCLASSIFIED

the quarter, recruiting more than a million new machines. Nearly half of all new botnet control servers were in the United States. The report also noted a dramatic increase in malware designed to attack mobile devices that run Android. It also found that most mobile malware originated in and targeted China and Russia. Malware targeting Apple computers also continued to rise steadily. Source:

http://www.computerworld.com/s/article/9227415/McAfee_reports_big_spike_in_malware

Yahoo strengthens mail filters after attempted JavaScript attack. Yahoo! strengthened its Web mail filters after researchers at Trend Micro detected a JavaScript attack the week of May 14 that was targeting its users. In the past, vulnerabilities within Web mail platforms were used to compromise accounts maintained by journalists and activists. May 18, Trend Micro said they detected several e-mails being used in targeted attacks that contained JavaScript in the “From” field. The code was attempting to launch a DOM-based cross-site scripting (XSS) attack, which would presumably yield access to the victim’s account to the attacker. Source:

<http://www.securityweek.com/yahoo-strengthens-mail-filters-after-attempted-javascript-attack>

Cross-browser worm spreads via Facebook, security experts warn. Malware writers used Crossrider, a cross-browser extension development framework, to build a click-fraud worm that spreads on Facebook, Kaspersky Lab researchers said May 21. Crossrider is a Javascript framework that implements a unified application programming interface (API) for building Firefox, Chrome, and Internet Explorer extensions. The API allows developers to write code that will run inside different browsers and, by extension, on different operating systems. The framework is still in beta testing and its creators plan on adding support for Safari soon. The new piece of malware is called LilyJade and is being sold on underground forums for \$1,000. Its creator claims the malware can infect browsers running on Linux or Mac systems, and since it does not have any executable files, no antivirus program is designed to detect it. The malware’s purpose appears to be click fraud. It is capable of spoofing rogue advertisement modules on Yahoo, YouTube, Bing/MSN, AOL, Google, and Facebook, a Kaspersky malware expert said. When users view or click on these ads, the malware’s creators earn money through affiliate programs. To spread, the malware leverages control over infected browsers to piggyback on active Facebook sessions and send spam messages on behalf of authenticated Facebook users. The links included in LilyJade’s Facebook spam direct users to compromised sites that load the Nuclear Pack exploit kit into a hidden iframe. Exploit kits like Nuclear Pack attempt to exploit vulnerabilities in outdated software — usually browser plug-ins like Java, Flash Player, or Adobe Reader — to infect computers with malware. Source:

http://www.computerworld.com/s/article/9227351/Cross_browser_worm_spreads_via_Facebook_security_experts_warn

Zeus Trojan variant comes with ransomware feature. The recent popularity of ransomware as a tactic for tricking users into paying money resulted in an unexpected malware combination. F-Secure researchers recently spotted a new Zeus 2.x variant that includes a ransomware feature. Once this particular piece of malware is executed, it first opens Internet Explorer and directs it toward a specific URL — [lex.creativesandbox.com/locker/lock\(dot\)php](http://lex.creativesandbox.com/locker/lock(dot)php). Simultaneously, the

UNCLASSIFIED

UNCLASSIFIED

users are blocked from doing anything on their computer. The site in question is offline, so it is difficult to be sure of what it contained, but a guess would be an extortion message. The command for “unlocking” the computer is present on the computer, in the registry, so it is possible to do so without paying the ransom. Source: http://www.net-security.org/malware_news.php?id=2120&utm

Social engineers breach billing service WHMCS. Thousands of passwords and credit card details were exposed online after social engineers breached the billing platform WHMCS. Attackers obtained the data after masquerading as the platform’s lead developer, and managed to con the company’s hosting provider to release administrator credentials. The developer’s details were then used to access WHMCS’s database and steal hashed customer credit card numbers and passwords, usernames, and support tickets. Along with that data, they also made public a 1.7GB cache that included the WHMCS control panel and Web site information. Almost a day’s worth of data was erased from the compromised servers, while links to the cache and other smaller files were hijacked. The lead developer said attackers from the group UGNazi provided correct answers to identity verification questions. Source: <http://www.scmagazineuk.com/social-engineers-breach-billing-service-whmcs/article/242176/>

NATIONAL MONUMENTS AND ICONS

(Utah) Hurricane wildfire burns 2,000 acres of southwestern Utah. Firefighters were gaining the upper hand on a wind-driven wildfire that had scorched an estimated 2,000 acres of southwestern Utah’s tinder-dry high desert. The fire, which began May 22, was burning in grass and sagebrush in hills that dot the area between Hurricane and Apple Valley. Nearby Highway 59 was closed for several hours as smoke billowed from the blaze, and flames were at one point moving toward homes in the Angel Heights and Rainbow Canyon areas in southeast Hurricane. However, winds shifted away from both the subdivision and highway, allowing traffic to resume and ending fears of a possible evacuation, public safety dispatchers said. “We’re calling it ‘human-caused,’ but don’t have specifics yet,” a Bureau of Land Management (BLM) spokesman said. In all, about 160 firefighters — a mix of BLM, Forest Service, Hurricane city, and local volunteer crews — fought the blaze through the night and into the morning. About half that number remained on the fire by the next morning. Crews had about 60-70 percent of their containment lines constructed by May 23. Source: <http://www.sltrib.com/sltrib/news/54168603-78/fire-hurricane-wednesday-utah.html.csp>

POSTAL AND SHIPPING

(California) APD detains arson suspect. Arcata, California detectives detained an unidentified woman May 21 after she allegedly confessed to setting a fire inside a post office lobby and attempting to set fire to a vehicle. Officers responded to a fire at the Arcata Post Office May 20, according to an Arcata Police Department (APD) press release. They found paper and debris was set on fire inside the lobby, the release said. A passerby noticed the fire and extinguished the flames using a fire extinguisher. The Arcata Fire Department responded and put out the remaining fire. The lobby received minor fire damage to two walls as well as smoke damage,

UNCLASSIFIED

UNCLASSIFIED

the police department said. May 21, the police department received a report of a person putting a lit cigarette into the fuel tank of a parked vehicle. Officers later located a woman who matched the suspect's description and she confessed to setting both fires. Source:

http://www.times-standard.com/breakingnews/ci_20681022/apd-detains-arson-suspect

(Michigan) Unknown white powder found on mailboxes. An unknown white powder covering mailboxes caused police and fire crews to close roads in the area of North Lakeview Drive and Beamish Road in Jerome Township, Michigan, May 21. "We have the area cordoned off and we have a team coming to test it," a Midland County Sheriff's Office captain said. The Jerome Township Fire Department was called to the scene when a resident discovered the white powder on and inside of a mailbox, the Jerome Township fire chief said. "A resident went out to ... his mailbox [and] discovered the powder substance on and in his mailbox. And then as we got here we discovered there was a multitude of them (mailboxes with powder). So we have actually isolated the whole area off and will start testing them now," the fire chief said. Agencies at the scene also included the Midland Saginaw Bay City HAZMAT team and Lincoln Township Fire Department. Source:

http://www.ourmidland.com/police_and_courts/article_f1d713d4-a34f-11e1-88d8-001a4bcf887a.html

PUBLIC HEALTH

(Wisconsin) Health officials urge residents to seek pertussis vaccine. With summer camps and other programs for children starting in the next few weeks, State health officials are urging Wisconsin residents to seek pertussis vaccinations, according to a Wisconsin Department of Health Services release issued May 22. Wisconsin is experiencing a widespread outbreak of the disease, with 1,514 confirmed and probable cases to date. "The best defense against pertussis continues to be vaccination," said the State health officer. "We recommend all Wisconsin residents check their vaccination status and schedule a visit to their healthcare providers if they have not yet been immunized against pertussis." Source:

<http://www.dhs.wisconsin.gov/News/PressReleases/2012/052212.htm>

TRANSPORTATION

Nothing Significant to Report

WATER AND DAMS

(Louisiana) Invasive plants clogging up vital bayou waterway, drinking water source. Invasive plants, like water hyacinths and hydrillas, are threatening Bayou Lafourche in Louisiana along Highway 308, the source of fresh water for more than 300,000 people in bayou communities, WWL 4 New Orleans reported May 18. "Salt water can intrude at the bottom of Bayou Lafourche and cause problems with drinking water," a spokeswoman from the Barataria-Terrebonne National Estuary Program said. The chairman of the Bayou Lafourche Fresh Water District also expressed concern. The combination of a lack of spraying the invasive plants and a

UNCLASSIFIED

UNCLASSIFIED

mild winter made matters worse in 2012. The U.S. Army Corps of Engineers did not spray the plants due to a lack of funding for the \$1.5 million program. In the long term, dredging the bayou could help, but such an effort is costly. In the short term, the water district is working to cut the plants. The water district applied for a \$20 million federal grant, which it hopes can help pay for dealing with the invasive plants. Source: <http://www.wvltv.com/news/local/Invasive-plants-clogging-up-vital-bayou-waterway-drinking-water-source-152098165.html>

(Hawaii) Kalapaki Beach remains closed following sewage spill. Kauai, Hawaii's Kalapaki Beach remained closed May 21, as water quality tests showed there were still signs of a sewage spill from May 16. A reported 400,000 to 500,000 gallons of treated effluent spilled into a storm drain that leads into Kalapaki Bay. Officials said the spill happened after a partial power outage at the Lihue Wastewater Treatment Plant due to a failure in an internal circuit that powered the newly-installed processes at the plant, which produces irrigation water. Most of the water is used at the Kauai Lagoons golf courses. Officials limited the production of irrigation water until a new alarm system to monitor power interruptions could be installed and tested at the treatment plant. Source: <http://www.hawaiinewsnow.com/story/18567936/three-days-after-sewage-spill-kalapaki-bay>

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:

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

UNCLASSIFIED