

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

Nothing Significant to Report

REGIONAL

(Montana) Hazardous chemicals found on parking lot pay boxes. Six parking-lot pay boxes in downtown Helena, Montana, were vandalized with an industrial-strength solvent June 14 or June 15 that also may have sent a pair of heavy-equipment operators, who may have been contaminated with the same chemical, to the hospital. A Helena police official said June 15 the Helena Parking Commission reported finding an unknown substance on six of the boxes that dispense tickets showing proof of payment for parking. A hazardous materials team from the Helena Fire Department determined the substance to be a powerful solvent. Later June 15, two people working on a utility project also came in contact with what appeared to be the same substance and went to the hospital for treatment of possible chemical burns. They were later released. Source: http://helenair.com/news/local/crime-and-courts/hazardous-chemicals-found-on-parking-lot-pay-boxes/article_51a5eb4a-b779-11e1-b82a-001a4bcf887a.html

(South Dakota) Family: Crew member dead in C-130 crash in SD. A military cargo plane from the North Carolina Air National Guard crashed July 1 while fighting a wildfire in the Black Hills of South Dakota, killing at least one of the six crew members aboard and forcing officials to ground the fleet. The family of one of the crew members confirmed they were notified early July 2 that he had died in the C-130 crash. The plane crashed after dropping fire retardant July 1, military officials said. Fall River County, South Dakota sheriff's officials said three crew members were taken to a hospital. All eight Air Force C-130s had been dispatched to Peterson Air Force Base, Colorado, the week of June 25 to fight Colorado wildfires, including the 28-square-mile Waldo Canyon Fire. Seven C-130s are being kept on the ground under an "operational hold," said a Northern Command spokesman. It was not immediately clear when they would resume work or what impact their absence would have on firefighting across the West. Source: <http://www.airforcetimes.com/news/2012/07/ap-peterson-c-130-crash-forest-fire-070212/>

(South Dakota) Salem water restored after dry spell in community. Salem, South Dakota, restored water service to its residents June 28. Residents in the city were told June 27 not to use tap water after a computer component failed and caused the city's water treatment plant to shut down. A replacement part was brought in June 28, said a finance officer. The part was installed, programming was completed, and the water tower was refilling after dropping dangerously low June 27 and June 28. The city asked for people not to water outside their home and businesses until June 30 to allow the system to fully refill. Source: <http://www.mitchellrepublic.com/event/article/id/67125/group/homepage/>

UNCLASSIFIED

NATIONAL

U.S. critical infrastructure cyberattack reports jump dramatically. U.S. critical infrastructure companies saw a dramatic increase in the number of reported cybersecurity incidents between 2009 and 2011, according to a new report from the U.S. Industrial Control System Cyber Emergency Response Team (ICS-CERT). In 2009, ICS-CERT fielded nine incident reports. In 2010, that number increased to 41. In 2011, it was 198. Of those 198, 7 resulted in the deployment of onsite incident response teams from ICS-CERT, and 21 of the other incidents involved remote analysis efforts by the Advanced Analytics Lab. Incidents specific to the water sector, when added to those that impacted multiple sectors, accounted for more than half of the incidents due to a larger number of Internet-facing control system devices reported by independent researchers, according to the report. Source: <http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/240003029/>

At least 22 dead after US storms cut power in East. Millions of people in a swath of States along the East Coast and farther west went into a third sweltering day without power July 2 after a round of summer storms that killed more than a dozen people. The outages left many to contend with stifling homes and spoiled food as temperatures approached or exceeded 100 degrees. Around 2 million customers from North Carolina to New Jersey and as far west as Illinois were without power, that was down from the more than 3 million homes and businesses that lost power shortly after the June 29 storm hit. Utility officials said the power would likely be out for several more days. Since June 29, severe weather was blamed for at least 22 deaths, most from trees falling on homes and cars. The power outages prompted concerns of traffic problems as commuters took to roads with darkened stoplights. There were more than 400 signal outages in Maryland July 2, including more than 330 in hard-hit Montgomery County outside the nation's capital, according to the State Highway Administration. There were 100 signal outages in northern Virginia late July 1, and 65 roads were closed, although most were secondary roads. Power crews from as far away as Florida and Oklahoma were headed to the mid-Atlantic region to help get the power back on. Source: <http://www.businessweek.com/ap/2012-07-02/at-least-22-dead-after-us-storms-cut-power-in-east>

Saudi student in Texas convicted of terrorism, former president a target. A U.S. federal jury in Texas convicted a Saudi Arabian citizen June 27 of attempting to use chemicals to build a weapon of mass destruction to attack several targets, including the Dallas home of a former U.S. President. The convict, who was a student at South Plains College near Lubbock, Texas, kept a journal that listed many targets. They included nuclear power plants, reservoir dams in Colorado and California, and hydroelectric stations. Evidence presented at his trial indicated he had been researching online how to construct an improvised explosive device, using several chemicals as ingredients, according to the U.S. Department of Justice. He purchased ingredients and conducted online research on his potential targets, said an assistant U.S. attorney. His plans were thwarted early in 2011, when a chemical supplier who had been contacted by him told the FBI he was worried about an attempted purchase of a compound called concentrated phenol, an ingredient in explosives. The convict was a legal resident of the United States, in the

UNCLASSIFIED

country on a student visa. He faces up to life in prison when he is sentenced in October. Source: <http://www.reuters.com/article/2012/06/27/us-usa-security-saudi-idUSBRE85Q1PG20120627>

INTERNATIONAL

Officials: Iranians targeted Israeli, US interests. Two Iranians who led authorities to a cache of explosives after their arrest planned to attack Israeli, U.S., British, or Saudi targets inside Kenya, officials said July 1. The two are believed to be members of Iran's Islamic Revolutionary Guards Corps Quds Force, an elite and secretive unit that acts against foreign interests, one of the officials said. Kenyan security forces arrested the Iranians June 19 and were then led to 33 pounds of RDX, a powerful explosive that could have been used against multiple targets or concentrated in one large bomb. If used together, the explosives could have leveled a medium-sized hotel, officials said. The two suspects appeared in a Kenyan court the week of June 25. Several resorts on Kenya's coast are Israeli-owned, as is Nairobi's largest and newest shopping mall. Source:

<http://www.google.com/hostednews/ap/article/ALegM5hBisIn3dEip7A8AQ6gWmk35iNfKw?docId=aab8faf2f8b042809c9779ceb5d4a4e7>

Avian influenza outbreak confirmed in Mexico. Mexican veterinary authorities confirmed the week of June 25 there was an outbreak of avian influenza near Guadalajara that caused the death of nearly a quarter million chickens since early June, and so far has forced a quarantine zone around three poultry processing facilities in the Mexican state of Jalisco. In a follow-up report submitted to the World Organization for Animal Health, Mexican animal health officials said intravenous pathogenicity tests revealed a highly pathogenic H7N3 subtype is the cause of the current outbreak. Mexican veterinary authorities are intensifying avian influenza control efforts in the region, which houses several large commercial farms. The event represents the first highly pathogenic avian influenza outbreaks in Mexican flocks since the country battled H5N2 in the mid 1990s. The outbreaks began at three farms in Jalisco state June 13, causing clinical signs in the layer flocks. The disease sickened 587,160 of more than 1 million susceptible birds, killing nearly 220,000 of them. Source: <http://southwestfarmpress.com/livestock/avian-influenza-outbreak-confirmed-mexico?page=1>

Two held in UK over fear of attacks before Olympics. Police arrested two men June 28 on suspicion of preparing terrorist attacks in Britain, less than a month before the opening of the London Olympic Games in the British capital. Seven years after suicide bombers killed 52 people in a string of coordinated attacks in London, British security forces are on high alert for any signs of trouble ahead of the Games, which start July 27. London police said the two men were arrested by officers from its Counter Terrorism Command on suspicion of terrorist-related activity. "Both (are) in custody at a central London police station," it said in a statement. Police and military strategists are gearing up for a range of security threats at the Olympics including bomb explosions, violent protests, and attacks using hijacked airliners. Source:

<http://www.reuters.com/article/2012/06/28/us-security-britain-idUSBRE85R12120120628>

UNCLASSIFIED

UNCLASSIFIED

Red alert status raised at La Mesa Dam. La Mesa Dam in Quezon City, Philippines, was on red alert as the dam's water level reached near spilling level June 18. Metropolitan Waterworks and Sewerage System (MWSS) personnel said the dam's water level was only 0.38 meter below its spilling level of 80.15. They warned residents surrounding the dam to expect flooding if rains continued. State weather bureau PAGASA said rains since June 17 in most parts of Luzon were caused by the southwest monsoon that was being enhanced by typhoon "Butchoy". Butchoy was moving northward at 22 kilometers per hour (kph) and was expected to exit the Philippine area of responsibility the night of June 18. Source: <http://www.abs-cbnnews.com/nation/metro-manila/06/18/12/red-alert-status-raised-la-mesa-dam>

China releases five year food safety plan. In another attempt to calm consumer fears, China released a 5-year plan the week of June 11 to upgrade its food safety regulations. According to the government, the plan by the country's ministry of health is aimed at revamping outdated standards, which includes "reviewing and abolishing any contradicting or overlapping standards" and writing new ones. The framework was announced on the heels of China's Food Safety Week. The plan calls for coordination between 14 different government departments — including the ministry of agriculture — to complete reviewing and revamping the existing standards by 2015. The plan admits the country "is still suffering from the absence of several major food safety regulations." "The government will prioritize safety standards for dairy products, infant food, meat, alcohol, vegetable oil, seasoning, health products and food additives so as to specify limits for dangerous ingredients in these foods," according to the release. "Moreover, the government will make special efforts to set standards for testing various contaminants, food additives, microorganisms, pesticide and animal drug residue in food production by 2015." Source: <http://www.foodsafetynews.com/2012/06/china-releases-five-year-food-safety-plan/>

BANKING AND FINANCE INDUSTRY

Fraud alert: Zeus malware steals banking details via fake login pages. Security experts from Threat Metrix and the United Kingdom's Action Fraud warned Internet users to be on the lookout for a new variant of the infamous Zeus malware that attempts to steal sensitive data by posing as genuine log-in pages, Softpedia reported July 5. The fraud starts with a normal log-in page, but once unsuspecting users enter their credentials, they are presented with a Web page that requests credit card information. In the case of social media sites, the victim is notified that by completing the form he can link his payment card to the account to make the acquisition of Facebook credits easier. This operation allegedly also offers enhanced security and even 20 percent cash back. The trojan is also able to adjust balances so victims are unaware of the fraudulent transactions. Customers of payment processors and companies from the retail industry are also at risk since most Web sites can be easily replicated, and for each situation the fraudsters can come up with apparently legitimate reasons for why the victim must provide credit card details. Source: <http://news.softpedia.com/news/Fraud-Alert-Zeus-Malware-Steals-Banking-Details-Via-Fake-Login-Pages-279372.shtml>

UNCLASSIFIED

UNCLASSIFIED

First wave of U.S. 'living wills' provides a blueprint for the industry. U.S. bank holding companies with \$250 billion or more in total nonbank assets and foreign-based bank holding companies with \$250 billion or more in total U.S. nonbank assets were due to submit resolution plans known as the "living wills" to the Federal Reserve and Federal Deposit Insurance Corporation (FDIC) July 2. The first wave of submissions included five of the biggest U.S. banks. Summarized public versions of the resolution plans were due to be released by July 3. The living wills are intended to provide road maps for regulators for the orderly unwinding of firms without spillover effects onto other parts of the economy and without costly bailouts. The firms will have to provide a detailed account of their business lines and legal entities, information systems, capital and cash flows, and an analysis explaining resolution options. The rule will allow the FDIC and the Federal Reserve to impose various restrictions on capital, leverage, or liquidity of the firm if the living wills are found to be deficient or non-credible. When warranted, the regulators will be able to curtail the firm's operations, and require divestiture of assets, though the FDIC made clear that this route would only be taken as a last resort. Source: <http://blogs.reuters.com/financial-regulatory-forum/2012/07/02/first-wave-of-u-s-living-wills-provides-a-blueprint-for-the-industry/>

U.S. targets informal banks for alleged aid to Taliban. The U.S. administration imposed sanctions on a pair of informal money-exchange networks in Afghanistan and Pakistan June 29 in what officials described as the first use of the tactic to attack the financial underpinnings of Taliban militants who rely on the system to fund their insurgency. The sanctions announced by the Treasury Department were coordinated with similar measures adopted by the United Nations as part of a broad effort to slow the flow of cash used by the Taliban to pay salaries and purchase weapons for attacks in Afghanistan. The informal cash networks — commonly known as hawalas — have long been used by Taliban commanders and other militants to move funds back and forth across the Afghan-Pakistani border, according to administration officials. The two hawalas were identified as the Haji Khairullah Haji Sattar Money Exchange and the Roshan Money Exchange. Treasury Department documents alleged that Afghan Taliban commanders maintained accounts in both networks and regularly withdrew thousands of dollars to pay off Taliban-backed "shadow" governors, buy weapons, and pay fighters' salaries. Source: http://www.washingtonpost.com/world/national-security/us-targets-informal-banks-for-alleged-aid-to-taliban/2012/06/29/gJQAWAInBW_story.html

Banking trojan harvests newspaper readers' credentials. Security firm ESET warned of financial malware trying to harvest usernames and passwords from a major newspaper's Web site, Information Week reported June 29. ESET said it observed financial malware known variously as Gataka and Tatanga being used in four recent attack campaigns. Targets include banks in Germany and the Netherlands, as well as an attack "trying to obtain accounts on a major U.S. newspaper's Web site by performing brute-force guesses of usernames and passwords," a malware researcher at ESET said. In all of the campaigns, ESET observed the malware connecting with between three and 10 different hacked Web pages, which served as proxies for the botnet's command-and-control server. The researcher estimated that the underlying botnet contained "somewhere between 20,000 and 40,000 infected hosts," with the vast majority of compromised PCs located in Germany. The Gataka malware itself was first detailed by S21sec in

UNCLASSIFIED

UNCLASSIFIED

February 2011. The security firm dubbed the trojan application, written in C++, as being “rather sophisticated” given its ability to hide on infected systems. It does that in part by downloading encrypted modules after it infects a system. According to S21sec, these modules or plug-ins offer additional functionality and are decrypted in memory when injected to the browser or other processes to avoid detection by antivirus software. Source:

<http://www.informationweek.com/news/security/vulnerabilities/240003004>

Buyer beware: Mobile payments might not be protected. Some current financial rules may not be fully up to the task of regulating the growing number of mobile payment systems, government officials told a House subcommittee June 29. The associate general counsel for the Federal Reserve Board of Governors warned members of the House Financial Services Subcommittee on Financial Institutions and Consumer Credit that in the broader regulatory scheme many mobile systems may not be covered, especially those used by people or organizations that are not banks. Mobile payments usually refer to making purchases, bill payments, charitable donations, or payments to other persons using a mobile device, with the payment applied to a phone bill, credit card, or withdrawn directly from a bank account. As mobile payment options have multiplied, however, concerns have been raised over ensuring the transactions are secure and private; and that consumers have recourse if something goes wrong. Source: <http://www.nextgov.com/mobile/2012/06/buyer-beware-mobile-payments-might-not-be-protected/56540/>

Data in possible credit card breach appears to be old. A batch of names, addresses, e-mails, and phone numbers of credit card customers around the world released June 18 indicated a breach of a payment processor, but the data appeared old, IDG News Service reported. A hacker nicknamed “Reckz0r” posted a link to the data dump on Pastebin, and wrote on Twitter he had “penetrated over 79 large banks” and holds 50GB of data on MasterCard and Visa cardholders. No card numbers were released, however. Attempts to reach some of the U.S. cardholders affected were unsuccessful, since many of the phone numbers were disconnected or incorrect. But another person on the list in Australia said the information was very old. The home address published for him is 7 years out of date, and an e-mail address published at least 4 years old, the man said in a phone interview. The majority of the data appeared to come from U.S. cardholders, although other people listed purportedly live in countries including Egypt, Cambodia, Israel, Turkey, Pakistan, and elsewhere. The data includes only five digits of the credit card numbers and no expiration dates or three-digit security codes. The mix of international addresses indicates the target could have been an international payment processor, according to the head of CloudeyeZ, a security consultancy. Source:

http://www.computerworld.com/s/article/9228222/Data_in_possible_credit_card_breach_appears_to_be_old

Automatic transfer system evades security measures, automates bank fraud. Trend Micro June 18 released a new report that identifies an Automatic Transfer System (ATS) that enables cybercriminals to circumvent many bank security measures and drain victims’ bank accounts without leaving visible signs of malicious activity. In the new whitepaper, “Automatic Transfer System, a New Cybercrime Tool”, Trend Micro examines the automatic transfer systems within

UNCLASSIFIED

UNCLASSIFIED

two well-known crime kits, Zeus and SpyEye. Automatic transfer systems are added to the various crime kits as part of the Webinject files. They arm criminals with the ability to move funds from a victim's account without them being aware. In short, while the victim is performing one type of action, the ATS is transferring money. "Various active ATSs currently found in the wild are being used by cybercriminals to conduct automated online financial fraud," the whitepaper explains. "These versions use a common framework. Their base code does not change from one version to another. New functionality has been introduced in more recent versions, however, in order to address new security measures". Source:

<http://www.securityweek.com/automatic-transfer-system-evades-security-measures-automates-bank-fraud>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

FDA announces the voluntary removal by industry of certain perfluorinated greaseproofing agents from the marketplace. The U.S. Food and Drug Administration (FDA) announced July 2, five perfluorinated substances used as greaseproofing agents were voluntarily removed from interstate commerce by their manufacturers. After recent studies raised safety concerns with one type of perfluorinated chemical, known as C8, FDA initiated a comprehensive review of the available data. The decision by the chemical manufacturers, including BASF Corporation, E. I. DuPont de Nemours & Co, and Clariant, means the affected products will no longer be sold for application on paper or paperboard intended for food contact use. This commitment is noted on the FDA's Inventory of Effective Food Contact Substance (FCS) Notifications. The agency will also conduct a market survey of food packaging to ensure these compounds are no longer used in material that comes in contact with human or animal food. Source:

<http://www.fda.gov/Food/NewsEvents/ConstituentUpdates/ucm309925.htm>

(Wyoming) Wildfire strains helium, oil flows. Federal fire officials reported July 1 the Fontenelle wildfire, burning on the Bridger-Teton National Forest in Sublette and Lincoln counties in Wyoming, placed "substantial strain on helium plant construction ... and oil/gas production." The fire, reported to have grown to more than 49,000 acres July 1, shut down gas, oil, and helium production, "causing significant economic impact," according to InciWeb.org. The shutdown is "delaying contributions to the nation's critical helium supply and employment of 300-plus construction workers," the report stated. July 1, the forest officials reported 427 firefighters were fighting the blaze, which was 5 percent contained. Low humidity and high winds fanned the fire, which was burning on national forest, Bureau of Land Management, State, and private land about 70 miles south of Jackson. Road closures extend from the forest boundary at the top of Bare Pass at Red Castles, west to North Piney Meadows and Tri Basin Divide, south to Cheese Pass, Mount Isabel and Red Park, east to the junction of LaBarge Creek Road and the forest boundary, and north to Bare Pass. Source:

http://www.jhnewsandguide.com/article.php?art_id=8720

DuPont says claims over herbicide hit the millions. DuPont, which introduced a herbicide in 2011 later linked to the deaths of thousands of trees, has begun processing claims for compensation that are running into the hundreds of millions of dollars, company officials said.

UNCLASSIFIED

UNCLASSIFIED

Some 30,000 homeowners, golf courses, municipalities, and landscapers across the country have submitted claims, DuPont's president for crop protection said, according to the New York Times, June 26. The formal deadline for submission was February 1, but a few are still trickling in and are being accepted, he added. DuPont has declined to estimate how many trees died from exposure to the herbicide, marketed under the name Imprelis, but tree experts said it was probably at least in the hundreds of thousands. Weeks after homeowners and lawn care professionals began applying the new product on lawns, golf courses, and cemeteries in spring 2011, many trees on those properties, primarily conifers, started turning brown and dying. By August, DuPont had pulled the chemical from the market, and the U.S. Environmental Protection Agency banned it shortly afterward. DuPont officials said they have set aside \$225 million for claims people have already submitted, and that the payout could eventually reach \$575 million. That does not include costs related to a class-action lawsuit filed by thousands of homeowners, landscapers, and others, consolidated in federal court in Philadelphia. Source: <http://www.nytimes.com/2012/06/27/us/dupont-says-claims-over-herbicide-hit-the-millions.html? r=1>

COMMERCIAL FACILITIES

(Michigan) Incendiary devices found near mall. Authorities in Livingston County, Michigan, want to know who put six homemade incendiary devices near a shopping mall July 2, sparking a small grass fire. The fire burned near Green Oak Village Place mall in Green Oak Township. Authorities said the devices were made from 2-liter bottles and chemicals, and all exploded. The fire and one device were near a newly built home. Two of the devices were found on mall property, and three were found in a home under construction. Source: <http://www.dailypress.net/page/content.detail/id/246572/Incendiary-devices-found-near-mall-.html?isap=1&nav=5046>

(California) Oakland: Bomb squad blows up suspicious device downtown. Authorities determined that a suspicious object rigged with wiring was a "well-made hoax device" after it was found June 28 in the Chinatown district of Oakland, California, police said. The Alameda County Bomb Squad blew up the device in a planned detonation. A Salvation Army employee found a large thermos that contained Styrofoam and copper wiring that was taped around a steel bar, said an Alameda County Sheriff's Office spokesman. Fearing it was an explosive device, the employee called Oakland police who then called in the county bomb squad. Authorities blocked off streets in the surrounding two-block area, which is part of Oakland's normally busy Chinatown district, and evacuated nearby residents and merchants, an Oakland police spokeswoman said. A bomb technician determined the thermos was fake and was rigged to look like an explosive that could be detonated remotely, said the county sheriff's spokesman. The Oakland fire hazardous materials response team assisted in the operation. Source: http://www.insidebayarea.com/oaklandtribune/localnews/ci_20963550/police-investigating-suspicious-package-blocking-traffic-downtown-oakland

UNCLASSIFIED

UNCLASSIFIED

COMMUNICATIONS SECTOR

FCC examining storm damage to area phone networks after 911 calls failed. The Federal Communications Commission (FCC) was looking into the damage that the massive storm that swept from the Midwest into the Northeast June 29 caused to wireless and landline phone networks in the mid-Atlantic, the Washington, D.C. Hill reported July 3. As of early July 2, 16 percent of cell towers in West Virginia were still disabled. Nearly 11 percent of Maryland's towers were down, as well as 9 percent in Virginia, and 3 percent in Washington, D.C., according to the FCC. Widespread power outages also caused problems for many 9-1-1 call centers in the region. Source: <http://thehill.com/blogs/hillicon-valley/technology/236133-fcc-looking-into-damage-to-phone-networks-from-storm>

Latest hacker dump looks like Comcast, AT&T data. A group of hackers posted to the Web June 27 data that appears to include Comcast employee names, ages and salaries, as well as e-mails and passwords associated with AT&T VoIP service accounts. Proclaiming the kickoff of “#WikiBoatWednesday ... when all the members from @TheWikiBoat fight corruption, leak data, and bring down websites,” the hackers released the data in two different posts to the Pastebin Web site. One of the Twitter handles used by the group is @AnonymousWiki but the connection to the larger, decentralized collective known as “Anonymous” is unclear. As with many data dumps, it is unclear whether the data is what the hackers claim it is, whether it is current, who actually stole it, and how. Source: http://news.cnet.com/8301-1009_3-57462403-83/latest-hacker-dump-looks-like-comcast-at-t-data/

CRITICAL MANUFACTURING

Innovage recalls Discovery Kids lamps due to fire and burn hazards. The U.S. Consumer Product Safety Commission, in cooperation with Innovage LLC, July 3 announced a voluntary recall of about 300,000 Discovery Kids Animated Marine and Safari Lamps. Consumers should stop using recalled products immediately unless otherwise instructed. The placement of internal wires near the circuit board can cause electrical short-circuiting and sparking, posing a fire and a burn hazard to consumers. Innovage has received 11 reports of short circuiting. This includes three reports of lamps catching fire, which led to property damage. The lamps were sold at Bed Bath and Beyond, Bonton, JCPenney, Kohls, Office Max, and Toys "R" Us stores nationwide as well as through online retailers from June 2010 through March 2012. Source: <http://www.cpsc.gov/cpsc/pub/prereel/prhtml12/12215.html>

Toyota to recall 154,000 Lexus SUVs to fix floor mat. Federal safety regulators said June 29 they asked Toyota to recall about 154,000 Lexus sport utility vehicles because their floor mats can trap the gas pedal and cause the vehicles to speed up without warning. The agency also said it may investigate whether Toyota told the agency about problems quickly enough. The move adds the 2010 model year Lexus RX 350 and RX 450 to other safety recalls dating to 2009. The National Highway Traffic Safety Administration said it requested the recall after reviewing complaints from customers and information from Toyota. The agency said people with the recalled vehicles should remove the driver's side floor mat and have their vehicles serviced

UNCLASSIFIED

UNCLASSIFIED

promptly. Source: <http://bottomline.msnbc.msn.com/news/2012/06/29/12482378-toyota-to-recall-154000-lexus-suvs-to-fix-floor-mat?lite>

Exhaust fans sold at Lowe's stores recalled due to fire hazard; Made by Delta Electronics Dongguan. The U.S. Consumer Product Safety Commission, in cooperation with Homewerks Worldwide and Delta Electronics (Dongguan), June 28 announced a voluntary recall of about 68,000 Harbor Breeze Bath Fans with Heater and Light. Consumers should stop using recalled products immediately unless otherwise instructed. The fan's heater blades can fail to rotate properly, causing the fan to overheat and posing a fire hazard. The firm has received 11 reports of the fan overheating with smoking or flames within the fan housing, including three reports of minor property damage. The recall involves plastic Harbor Breeze bathroom fans with a center light and a heater. The fans were sold at Lowe's stores nationwide and on Lowe's Web site from September 2010 through March 2012. Source: <http://www.cpsc.gov/cpscpub/prereel/prhtml12/12212.html>

Ceiling mounted light fixtures recalled by Thomas Lighting due to fire and shock hazards. The U.S. Consumer Product Safety Commission, in cooperation with Thomas Lighting, June 19 announced a voluntary recall of about 83,750 Thomas Lighting ceiling flush mount light fixtures. Consumers should stop using recalled products immediately unless otherwise instructed. The fixture's socket wire insulation can degrade, leading to charged wires becoming exposed, causing electricity to pass to the metal canopy of the fixture. This poses a fire and electric shock hazard to consumers. Thomas Lighting has received 11 reports of defective fixtures that resulted in the home's Arc Fault Circuit Interrupter (AFCI) tripping. The recall involves 28 different models of ceiling flush-mounted light fixtures manufactured between June 1, 2010 and November 25, 2010. Source: <http://www.cpsc.gov/cpscpub/prereel/prhtml12/12197.html>

Toyota fire probe expanded to 1.4 million autos. Federal safety investigators broadly expanded an investigation into a potential fire hazard that now involves about 1.4 million Toyota cars and sport utility vehicles, the Detroit Bureau reported June 18. According to the National Highway Traffic Safety Administration (NHTSA), the automaker is looking into reports the window switches on the driver's side doors of a number of different Toyota models can overheat and catch fire. The problem has so far been linked to 161 fires and 9 injuries. The Toyota probe was initially launched in February and covered 800,000 2007 Camrys and RAV4s. Toyota's practice of making widespread use of common components caused the NHTSA to add an additional 800,000 vehicles, including some Yaris subcompacts from the 2007 to 2009 model years, as well as the 2008 Highlander Hybrid run. The NHTSA also expanded the probe to cover Camrys produced in the 2008 and 2009 model years. Source: <http://bottomline.msnbc.msn.com/news/2012/06/18/12279930-toyota-fire-probe-expanded-to-14-million-autos?lite>

DEFENSE/ INDUSTRY BASE SECTOR

New version of Sykipot trojan linked to targeted attacks on aerospace industry. According to researchers at the security firm AlienVault, a new version of the Sykipot trojan is being pushed

UNCLASSIFIED

UNCLASSIFIED

to unsuspecting users in a wave of online attacks, including targeted attacks on attendees of an international aerospace conference, Threatpost reported July 3. The attacks use exploits for recently disclosed security holes, such as Microsoft's Windows XML Core Services vulnerability first disclosed in June. The new Sykipot variant also uses a collection of recently registered Web domains to issue malicious attacks. Most were registered in the last month and are linked to the same yahoo.com e-mail address, AlienVault disclosed. At least one of the new domains was linked to targeted phishing-email attacks on attendees of the IEEE Aerospace Conference (the International Conference for Aerospace Experts, Academics, Military Personnel, and Industry Leaders), AlienVault said. Source: http://threatpost.com/en_us/blogs/new-version-sykipot-trojan-linked-targeted-attacks-aerospace-industry-070312

Aging U.S. atomic shipping gear poses concern, auditors find. The old age of the U.S. Energy Department's highly protected atomic-transport automobiles is one of "several" major hurdles faced by its Secure Transportation Office, the department's inspector general said in an assessment issued June 29. "Based on its own criteria, [the Secure Transportation Office's] entire fleet of armored tractors is beyond its operational life as of December 2011," the Knoxville News Sentinel quoted the department's auditors as saying in the analysis. U.S. nuclear-warhead sustainment efforts and transfers of arms production components are set to substantially boost the need for closely guarded atomic transports over the coming 84 months, the assessment states. The Secure Transportation Office has satisfied a majority of transfer needs to date, though, and its capabilities are projected to remain sufficient, according to the findings. Other concerns "include maintaining the reliability of existing equipment; ensuring that future federal agent overtime levels are consistent with safe operations; and, validating essential resource planning data," an assessment abstract states. "Accordingly, management attention is needed to address these challenges to reduce the risk that [the Secure Transportation Office] will be unable to meet its future mission requirements." Source: <http://www.nti.org/gsn/article/aging-us-atomic-shipping-gear-poses-concern-audit/>

Unencrypted GPS lets hackers take control of drones. Using only \$1,000 worth of equipment, a group of researchers from the University of Texas at Austin hijacked a small drone, highlighting the vulnerabilities of unencrypted GPS signals, Discover Magazine reported July 1. While the powerful military drones used overseas use encrypted GPS signals, the ones in the United States rely on signals from open civilian GPS, which makes them vulnerable to GPS "spoofing." The head of the university's Radionavigation Laboratory and his team put on a demonstration for representatives of the Federal Aviation Administration and the DHS. To take control of the drone, the research group generated a fake GPS signal to match the real one, and then used the fake signal to overwhelm the real one, placing the drone under their control. The lead researcher predicts there could be as many as 30,000 drones patrolling the skies by 2020 and recommends investment in some resources in the authentication of civilian GPS signals. Source: <http://blogs.discovermagazine.com/80beats/2012/07/01/unencrypted-gps-lets-hackers-take-control-of-drones/>

FBI: High-tech economic espionage a vast, expanding threat. Driven by the general ease of stealing electronically stored data and the reality of growing global businesses, U.S. companies

UNCLASSIFIED

UNCLASSIFIED

lost some \$13 billion through economic espionage in the current fiscal year — and the problem is growing. Those observations were made the week of June 25 by the FBI during a House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence hearing. Testimony went on to add that as the FBI's economic espionage caseload is growing, so is the percentage of cases attributed to an insider threat, meaning that individuals currently (or formerly) trusted as employees and contractors are a growing part of the problem. An FBI assistant director for its counterintelligence division cited as an example a February 2012 indictment where several former employees with more than 70 combined years of service to a company were convinced to sell trade secrets to a competitor in the People's Republic of China. "The theft of U.S. proprietary technology, including controlled dual-use technology and military grade equipment, from unwitting U.S. companies is one of the most dangerous threats to national security," said the assistant director of national security investigations at U.S. Immigration and Customs Enforcement, who also testified. Source: <http://www.networkworld.com/community/node/80938>

United Technologies sent military copter tech to China. United Technologies Corp and two of its subsidiaries sold China software enabling Chinese authorities to develop and produce their first modern military attack helicopter, U.S. authorities said June 28. At a federal court hearing in Bridgeport, Connecticut, United Technologies and its two subsidiaries, Pratt & Whitney Canada and Hamilton Sundstrand Corp, agreed to pay more than \$75 million to the U.S. government to settle criminal and administrative charges related to the sales. As part of the settlement, Pratt & Whitney Canada agreed to plead guilty to two federal criminal charges — violating a U.S. export control law and making false statements. The charges were in connection with the export to China of U.S.-origin military software used in Pratt & Whitney Canada engines, which was used to test and develop the new Z-10 helicopter. Also as part of the deal, United Technologies and Hamilton Sundstrand admitted to making false statements to the U.S. government about the illegal exports. Hamilton Sundstrand and Pratt & Whitney Canada also admitted they failed to make timely disclosures, required by regulations, to the U.S. State Department about the exports. Source: <http://www.reuters.com/article/2012/06/28/us-usa-china-helicopters-idUSBRE85R1AG20120628>

EMERGENCY SERVICES

(Illinois) Hacker may have targeted Lemont's tornado sirens. Lemont, Illinois police suspect someone hacked into the village's tornado siren system, causing all seven sirens to sound for about 30 minutes, the police chief said July 3. Three sirens were activated inexplicably in Evanston June 30, including two at fire stations, officials said. "Those sirens can only be triggered by our 911 dispatch center," said the city's division chief of life safety services. "It's not something that just anyone can do. We're not certain on the source." Source: http://articles.chicagotribune.com/2012-07-03/news/chi-police-hacker-lemont-tornado-siren-20120703_1_tornado-sirens-sound-warning-radio-signal

(Oklahoma) Paramedics kept waiting in emergency rooms a growing problem. On any single day, 20 percent of the Emergency Medical Services Authority (EMSA) paramedics needed to

UNCLASSIFIED

UNCLASSIFIED

respond to emergencies in Tulsa, Oklahoma, could be stranded waiting in a hospital emergency room instead, the Tulsa World reported July 2. The State Medical Control Board is gathering data on a growing problem known as “bed delay,” which keeps ambulance crews tied up at hospital emergency rooms because no beds are available for the patient they have transported. A snapshot of data showed that in some cases, half a dozen ambulances out of about 30 normally on the streets of Tulsa were stranded at hospitals for more than an hour due to bed delays, said the medical director of the medical control board. He said the EMSA will record data on all situations in which an ambulance crew waits more than 15 minutes to transfer care of a patient to hospital staff. The data will be shared with hospitals and used to begin a discussion in the medical community about how to limit bed delays. While hospitals in some cities have been fined to discourage bed delays, he believes the issue can be addressed with communication and teamwork. Source:

http://www.tulsaworld.com/site/printerfriendlystory.aspx?articleid=20120702_11_A1_CUTLIN612976&PrintComments=1

Bomb threat app puts crucial data in responders’ hands. A new app for first responders, called the First Responder Support Tools (FiRST), designed by the U.S. Department of Homeland Security’s Science and Technology Directorate and partners, is a computer and smartphone app that attempts to provide details pertinent to bomb threats like potential blast radius, location of nearby schools and hospitals, evacuation routes, and suggested roads to be blocked off, Emergency Management reported June 28. In addition to geospatial data, the app also includes HAZMAT response information based on the Emergency Response Guidebook, which includes data on more than 3,000 hazardous materials. The app can retrieve current and forecasted weather data to show downwind protection zones for materials that are considered inhalation hazards. Once the user has all the information garnered by the app, they can e-mail a text summary, map image, and GIS file to colleagues. Source:

<http://www.emergencymgmt.com/safety/Bomb-Threat-App-Data-Responders.html>

ENERGY

(Texas) Copper theft leaves thousands without power. Thousands of people were left without power after copper thieves hit an American Electric Power (AEP) substation in Corpus Christi, Texas, July 2. An AEP spokesman said the wire stolen was the ground wire that lead up to the transformers. Because of the location of the wires, they had to shut off power for about 4,100 customers so they could repair it. An AEP spokesperson said the substations are already fairly secure, but AEP will look at how the thieves got in to see if any more changes must be made. Source: <http://www.kztv10.com/news/copper-theft-leave-thousands-without-power/>

500,000 customers still without power after storms. Six days after violent storms hit the United States, more than 500,000 homes and businesses remained without power from Ohio to Virginia as a heat wave baked much of the nation July 5. Nearly a third of electricity customers in West Virginia, home to 1.9 million people, were without power, making it the hardest hit State. Utilities warned that some people could be without power for the rest of the week in the worst-hit areas. Temperatures in Charleston were expected to reach 95 degrees and top 100

UNCLASSIFIED

UNCLASSIFIED

degrees July 6-7. The storms crossed the eastern United States with heavy rain, hail and winds reaching 80 miles per hour June 29, leaving more than 4 million homes and businesses without power, and the record heat that followed has killed at least 23 people. Source:

<http://www.reuters.com/article/2012/07/05/us-usa-weather-power-idUSBRE8640QK20120705>

(North Carolina) NC lawmakers OK tougher plant protest penalties. The North Carolina legislature agreed to give police authority to charge protesters at North Carolina utility plants with felonies if they attempt to disrupt plant operations or place themselves or others at risk of injury. The senate gave final legislative approval July 2 to legislation increasing penalties for first-degree trespass when they occur at power and water treatment plants. The measure was in response to the arrests of Greenpeace protesters at a coal-fired Duke Energy plant in Arden. Some protesters climbed a smokestack and others secured themselves to equipment. First-degree trespassing is currently a misdemeanor with a maximum 60 days in jail. The bill creates a higher grade of misdemeanor and a low-grade felony that could mean several months behind bars for a first offense. Source: <http://www.sfgate.com/news/article/NC-lawmakers-OK-tougher-plant-protest-penalties-3679491.php>

(Kentucky) Copper theft knocks out power for some customers. A Kentucky Utilities (KU) official said electricity was knocked out for more than 1,200 customers in central Kentucky after copper was stolen from a power substation June 28. A KU spokeswoman said power was expected to be restored to the customers June 28. The spokeswoman said the outage affected 1,225 customers in the Bloomfield and Fairfield areas in Nelson County. She said someone broke into the substation and stripped away copper wires. Source:

<http://www.fox19.com/story/18908570/copper-theft-knocks-out-power-for-some-customers>

Large, humanmade quakes rare, new government report concludes. The Associated Press reported June 16 that a major government science report concluded the controversial practice of hydraulic fracturing to extract natural gas does not pose a high risk for triggering earthquakes large enough to feel, but other types of energy-related drilling can make the ground noticeably shake. In more than 90 years of monitoring, human activity has been shown to trigger only 154 quakes, most moderate or small, and only 60 of them in the United States, the National Research Council report found. Most were caused by gas and oil drilling the conventional way, river damming, deep injections of wastewater, and purposeful flooding. Two other instances — a magnitude 2.8 tremor in Oklahoma and a 2.3 magnitude quake in England — can be attributed to hydraulic fracturing, a specific method of extracting gas by injection of fluids commonly referred to as “fracking,” the report said. The report shows that most of the tremors that can be blamed on humans occurred in California, Texas, Colorado, Oklahoma, and Ohio. California and Oklahoma had the biggest human-made shakes as byproducts of conventional oil and gas drilling. Colorado had three 5.0 to 5.5 man-induced quakes because of an injection well. Northern California has had 300 to 400 tiny quakes a year since 2005 because of geothermal energy extraction. Source:

<http://durangoherald.com/article/20120617/NEWS03/706179937/-1/s>

UNCLASSIFIED

FOOD AND AGRICULTURE

China reports bird flu outbreak. Authorities in China's remote northwestern region of Xinjiang culled more than 150,000 chickens following an outbreak of bird flu, officials said. The outbreak of the H5N1 strain of avian flu initially killed 1,600 chickens and sickened about 5,500, the agriculture ministry said July 2. In an effort to contain the disease, agricultural authorities quarantined the area and culled 156,439 chickens, according to the ministry. The outbreak occurred June 20 but was only confirmed as H5N1 bird flu July 2. The ministry said the outbreak happened at a farm run by the Xinjiang Production and Construction Corps. China is considered one of the nations most at risk of bird flu epidemics because it has the world's biggest poultry population, and many chickens in rural areas are kept close to humans. Source:

<http://www.google.com/hostednews/afp/article/ALeqM5iPIMCXigI97QkMnK4c9ZcLO6FTIA?docId=CNG.6570597d3c3999dd02f1b742aba26d6c.251>

Heat, dryness slam crop conditions — USDA. The quality of the nation's corn and soybean crops decreased the week of June 25, according to the July 2 U.S. Department of Agriculture (USDA) Crop Progress report. The amount of that crop in good to excellent conditions went from 58 percent to 48 percent. All that slide was taken up by the very poor and poor condition categories, with 7 percent of the crop in the former and 15 percent in the latter, the USDA said. Soybean conditions saw an 8 percent drop in the good and excellent categories over the week of June 18. Farmers said they are starting to find crop conditions that are deteriorating beyond repair, even if the weather trend reverses and turns cooler and wetter later in July. Source:

http://www.agriculture.com/news/crops/heat-dryness-slam-crop-conditions-usda_2-ar25028

US pasture conditions get even worse. Pasture conditions across the Plains, Midwest, and several other States worsened from already poor ratings the week of June 25, Dow Jones Newswires reported July 2. The U.S. Department of Agriculture rated nearly two-thirds of pasture acres on average across Indiana, Kentucky, Tennessee, Illinois, Missouri, and Kansas at poor to very poor. The latest ratings compared with an average of nearly 49 percent in the two categories in the week of June 18. Areas of severe drought stretch into Nebraska, Arkansas, and western States. For the 48 continental states, 43 percent of pasture acres rated poor to very poor, compared with 34 percent a year ago when the southwest was hit particularly hard.

Source: http://www.agriculture.com/news/livestock/us-pasture-conditions-get-even-wse_3-ar25029

Dole Fresh Vegetables announces precautionary recall of limited number of salads. Dole Fresh Vegetables voluntarily recalled 2,598 cases of bagged salad, the U.S. Food and Drug Administration (FDA) reported June 29. The product recalled is Dole Hearts of Romaine due to a possible health risk from *Listeria monocytogenes*. The salads were distributed in nine U.S. States: Alabama, Florida, Georgia, Maryland, North Carolina, Pennsylvania, South Carolina, Tennessee, and Virginia. The precautionary recall notification was issued due to an isolated instance in which a sample of Dole Hearts of Romaine salad yielded a positive result for *Listeria monocytogenes* in a random sample test conducted by the FDA. Source:

<http://www.fda.gov/Safety/Recalls/ucm310329.htm>

UNCLASSIFIED

Stink bug crisis reaches 38 states, Pacific Coast. The Chinese-exported stink bug crisis that ruined apple, peach, and grape harvests up and down the East Coast has now reached 38 states and the Pacific Coast, prompting the U.S. Congress to push the Agriculture Department to speed up the search for an assassin of the “brown marmorated stink bug.” Mid-Atlantic apple growers alone are reporting losses of nearly \$40 million a year, and now there are reports from Oregon’s orchards that the bug has landed there. Agriculture officials are studying the use of a miniscule Chinese bee to control the stink bug population. The bee lays its eggs in stink bug eggs, killing them. Source: <http://washingtonexaminer.com/stink-bug-crisis-reaches-38-states-pacific-coast/article/2501143>

Miramichi E. coli outbreak linked to romaine lettuce. Romaine lettuce was determined to be the likely source of an E. coli outbreak in Miramichi, New Brunswick, Canada, in April. Canada’s Department of Health released results of a case control study June 29 that examined 55 people. The study looked at what the people ate to determine if there were any patterns. The chief medical officer of health said all of those in the study who were sick with E. coli appear to have consumed romaine lettuce. The experts focused on the food items eaten by those who ate at Jungle Jim’s in Miramichi April 23-26. The federal agency became aware that cases matching the E. coli strain involved in the Miramichi outbreak had also been identified in Quebec and California, according to the province’s statement. Source: <http://www.cbc.ca/news/canada/new-brunswick/story/2012/06/29/nb-e-coli-miramichi-lettuce-1033.html>

Drought area larger than last year, losses may rival 1988. The historic drought in 2011 in the southwest gained a lot of attention for its impact on people, livestock, and wildlife, Drovers CattleNetwork reported June 29. The 2012 drought, however, is worse in many ways and likely to be more expensive to both agriculture and to consumers. According to the National Drought Mitigation Center, 72 percent of the continental United States is classified as “abnormally dry” or worse. By comparison, at the end of the third week in June 2011 just 32 percent of the continental United States was classified as “abnormally dry” or worse. Some meteorologists are comparing 2012 to the drought of 1988, which was estimated to cost American agriculture \$78 billion. The 2011 drought had a big impact on the U.S. cattle industry and strained the financial resources of many ranchers. The 2012 drought, however, will hit consumers much harder due to the impact it has already had on corn and soybean production. Crop forecasters are adjusting their estimates for the harvest, and smaller corn and soybean yields mean higher prices for many food items for American consumers. Source: <http://www.agprofessional.com/news/Drought-area-larger-than-last-year-losses-may-rival-1988-160733755.html>

UNCLASSIFIED

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

Backup systems ensured continuity of military networks during storm. A spokeswoman for the Defense Information System Agency (DISA) said the June 29 storms, which ravaged the Midwest and East Coast and knocked out power to 2 million people, briefly interrupted data center operations in Columbus, Ohio, and knocked out power to its headquarters at Fort Meade, Maryland. But backup power systems in Columbus quickly picked up the load until commercial power could be restored. Fall-over to alternative systems at Fort Meade and Columbus “was immediate and service was unaffected,” she said. Amazon Web Services, a commercial cloud provider angling for federal business with the launch of a government cloud in August 2011, lost both primary and backup power June 29, with full restoration of service June 30. When government officials consider the merits of commercial clouds versus internal data centers, they also must factor in issues such as continuity of service and backup capacity along with efficiency and economy, said an information technology consultant and retired U.S. Air Force brigadier general who did a tour at the DISA. Source: <http://www.nextgov.com/cloud-computing/2012/07/backup-systems-ensured-continuity-military-networks-during-storm/56587/>

(Arizona) Suspicious package forces evacuation. For the second time during the week of June 11, Tucson, Arizona police investigated a suspicious package delivered to a Department of Homeland Security Customs and Border Protection management office June 15. Office workers opening the package became concerned about its contents and notified federal police officers, a police official said. Tucson police had the building evacuated. Its bomb squad and special investigations unit responded, she said. June 11, two suspicious packages arrived at the office. Police determined they contained no explosives or chemicals. Source: http://azstarnet.com/news/local/crime/suspicious-package-forces-evacuation/article_4811a796-b76e-11e1-b59f-001a4bcf887a.html

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

DNSChanger victims to lose internet on Monday. July 9, the FBI will turn off the DNS server that currently intercepts queries from DNSChanger victims. This means users infected with the malware will be almost completely unable to access the Internet normally. Therefore, users are advised to check whether their computers or routers use one of the FBI-listed IP addresses for DNS queries by visiting dns-ok.us. Users can also check their configuration manually by looking for an IP within several address ranges. If an address from one of the ranges is already set as the DNS server on the computer or router, it is infected with DNSChanger. Users can find out where to locate this DNS server information for their particular case using a wizard set up by the eco association. Future DNS queries can be made using servers such as Google's at 8.8.8.8. Source: <http://www.h-online.com/security/news/item/DNSChanger-victims-to-lose-internet-on-Monday-1632475.html>

UNCLASSIFIED

Phonebook-slurping, spam-sending app found in App Store. A malicious application that steals mobile users' phonebooks and uploads them to a remote server was spotted on Google Play and Apple's App Store. Kaspersky Lab researchers first thought they were detecting an SMS worm, but after analyzing the "Find and Call" app, they discovered it was a trojan. It asks for permission to access user contacts. Once the phonebook is exfiltrated to the server, SMS spam messages containing a link to a page where the free app can be downloaded are sent to all the contacts, inviting them to use it to reach the sender. "It is worth mentioning that the 'from' field contains the user's cell phone number. In other words, people will receive an SMS spam message from a trusted source," said the researchers. "Malware in the Google Play is nothing new but it's the first case that we've seen malware in the Apple App Store," they noted. The Web site of this app allows users to supposedly access their social network accounts, mail accounts, and even their PayPal account. However, by adding money to the PayPal account, they are actually transferring it to a company based in Singapore, Malaysia. Both Google and Apple were notified and removed the app from their markets. Source: http://www.net-security.org/malware_news.php?id=2174&utm_source=feedburner&utm_medium=fee

Windows 8 has larger attack surface than Windows 7, researcher warns. The attack surface in Windows 8 is bigger than in Windows 7 because of new components and changed processes, especially with the Metro interface, warns a McAfee researcher. "Security risks from rogue applications and vulnerabilities in applications that interact with the web and handle user data leave lots of room for exploitation — not to mention ever-present malware on the desktop", he explained. At the same time, Windows 8 has additional security features, which include improvements to Windows anti-malware components, declarative resource access, application vetting via the Microsoft Store, and restrictive resource access for applications. Source: <http://www.infosecurity-magazine.com/view/26727/>

DNSChanger trojan still in 12 percent of Fortune 500. Any systems still infected with the DNSChanger trojan will be summarily disconnected from the rest of the Internet July 9. According to Internet Identity, this malware is still a resident on systems at roughly 4 percent of U.S. federal agencies and 12 percent of Fortune 500 companies. The latest stats from the DNSChanger Working Group (DCWG), an industry consortium working to eradicate the malware, more than 300,000 systems are still infected. That number is likely conservative: The DCWG measures infections by Internet protocol (IP) addresses, not unique systems. Because many systems that are on the same local network often share the same IP address, the actual number of DNSChanger-infected machines is probably quite a bit higher than 300,000. DNSChanger may no longer be hijacking search results, but the malware still carries secondary threats and risks. It was frequently bundled with other malicious software and disables antivirus protection on host machines. Source: <http://krebsonsecurity.com/2012/06/dnschanger-trojan-still-in-12-of-fortune-500/>

New crimeware bot Zemra behind DDoS attacks. Zemra, a new crimeware bot that shares traits with the banking trojans Zeus and SpyEye, has been making the rounds lately, according to a recent post on Symantec's Security Response blog. In the post, a Symantec researcher claims Zemra has been seen executing distributed denial-of-service (DDoS) attacks against

UNCLASSIFIED

UNCLASSIFIED

organizations and aiming to extort funds as of late. Like Zeus and SpyEye before it, Zemra's Web-based command and control panel is hosted on a remote server, allowing it to distribute commands to vulnerable computers. The bot is also capable of dynamically updating itself, monitoring devices, downloading and executing binary files, and spreading through USB devices, among other functions, Symantec said. Source:

http://threatpost.com/en_us/blogs/new-crimeware-bot-zemra-behind-ddos-attacks-062712

Citadel trojan upgraded to prevent virtual machine analysis. S21sec experts detected two major improvements implemented by malware authors for the Citadel trojan. Its encryption algorithm is changed, but it was also fitted with a mechanism that detects if it is executed inside a virtual machine or a sandbox. The enhancements were already seen in the wild, but they were also advertised on a Russian underground forum. The anti-emulator function is described as being able to protect the botnet against those who might want to perform reverse engineering on them. When the malware is executed, it checks to see if it is run inside applications such as CWSandbox, VMware, or Virtualbox. If it detects their presence, it does not remove itself and it does not stop from working. Instead, it begins to operate in a surreptitious manner. The trojan creates a fake domain name and attempts to connect to it. This strategy should fool the researchers into believing that the command and control (C&C) server cannot be reached and that the bot is dead. By closing all the processes related to VMware, such as vmwareuser.exe and vmwaretray.exe, experts forced the malware to begin working normally and to connect to the real C&C server. Source: <http://news.softpedia.com/news/Citadel-Trojan-Upgraded-to-Prevent-Virtual-Machine-Analysis-278073.shtml>

Encoding malicious PDFs avoids detection. A security researcher discovered attackers can thwart detection by most common anti-virus software if they encode malicious PDF files in the XDP format. XDP is an XML-based file format that includes the PDF as a Base64-encoded data stream. XDP files are opened by Adobe Reader just like a normal PDF would be and can therefore infect systems in the same way. The researcher's test document, which uses a 2-year-old security vulnerability in Adobe Reader, was only detected by one anti-virus package in his tests. After experimenting with the XDP format, he was able to create another file that fooled all 42 anti-virus engines used on VirusTotal. The exploit the researcher used has long since been patched. To make sure their networks are not attacked, users should avoid XDP files in general until Adobe patches its software or the anti-virus companies fix their detection methods, experts said. Source: <http://www.h-online.com/security/news/item/Encoding-malicious-PDFs-avoids-detection-1620310.html>

NATIONAL MONUMENTS AND ICONS

(Wyoming) Wyoming wildfires 'striking' in magnitude. Crews faced erratic winds and dry, fire-fueling conditions in Wyoming, July 2 as they fought three large forest fires that forced hundreds of evacuations across the State. At 82,000 acres, the Arapaho fire southwest of Wheatland was the largest of those burning in the State, and it destroyed an unknown number of structures as it remains too dangerous to allow a detailed assessment, according to information on a federal Web site. It was 10 percent contained by July 2. The sheriff's office

UNCLASSIFIED

UNCLASSIFIED

ordered the evacuation of Cottonwood Park, Friend Park, North Laramie Trailhead, and Harris Park. Many Forest Service trails and facilities in the area were closed. The Federal Emergency Management Agency announced it approved the use of federal funds to help cover the costs of fighting the Squirrel Creek Fire, which burned 7,000 acres about 30 miles southwest of Laramie, prompting new evacuations after a storm pushed flames west July 2, said a U.S. Forest Service representative. An area extending from the community of Jelm, north on both sides of Sheep Mountain to Highway 130 was evacuated. Albany County sheriff's officials also evacuated cabins and homes within 3 miles of Fox Park July 2. The Fontenelle Fire, about 17 miles west of the western community of Big Piney, burned more than 52,000 acres in Sublette and Lincoln counties. It was 8 percent contained. Source:

http://www.wyomingnews.com/articles/2012/07/03/news/20local_07-03-12.

(Utah) Official says more resources could have controlled Seeley Fire early. A fire prevention specialist said the Seeley Fire in Utah could have been stopped, the Salt Lake Tribune reported June 27. The fire prevention specialist for the Manti-La Sal National Forest said when the Seeley Fire ignited June 26, a hand crew and a helicopter were fighting it. However, the helicopter was called away to help with the Wood Hollow Fire on the other side of the mountain in Sanpete County. Soon the Seeley Fire, which was suspected to have been caused by lightning, was too much for the hand crew. With more aircraft, the fire could have been stopped that day, he said. Instead, the Seeley Fire grew to 9,000 acres June 27 and State Road 31, one of Utah's most-scenic drives, is scarred. Containment was reported at zero. Residents were ordered out of Scofield, Clear Creek, and Hiawatha. Boy Scouts and girls camps were evacuated, and the State park around Scofield reservoir was closed. Source:

<http://www.sltrib.com/sltrib/news/54390763-78/fire-jensen-wednesday-seeley.html.csp>

POSTAL AND SHIPPING

Nothing Significant to Report

PUBLIC HEALTH

FDA lays out new system to track medical devices. July 3, the Food and Drug Administration (FDA) proposed a new system to better track high-risk medical devices after they have gone public, giving patients, doctors, regulators, and consumer advocates access to data about specific products. Every high-risk medical device will be labeled with a unique identification code in an effort the FDA said will improve patient safety. Called a Unique Device Identifier (UDI), the code would provide basic information about the device, such as the name of the manufacturer, the type of device, the model of the device, and an expiration date. It could also include a batch or lot number to help officials better track recalled devices. That data will be stored in a UDI database that is accessible to the public, although no identifying patient information will be included. The FDA plans to phase in the system over 7 years, focusing on the highest-risk medical devices first. Source:

<http://www.postbulletin.com/news/stories/display.php?id=1501658>

UNCLASSIFIED

UNCLASSIFIED

Measuring the uncertainties of pandemic influenza. A major collaboration between U.S. research centers has highlighted three factors that could ultimately determine whether an outbreak of influenza becomes a serious epidemic that threatens national health, Infection Control Today reported July 2. Researchers from Argonne, Los Alamos, and Sandia National Laboratories, and the National Renewable Energy Laboratory, used sensitivity analysis to uncover the most important disease characteristics pertaining to the spread of infection with an influenza virus. These are the fraction of the transmission that occurs prior to symptoms, the reproductive number, and the length of each disease stage. Their use of data from past pandemics as well as information on potential viral evolution demonstrates that current response planning may underestimate the pandemic consequences significantly. Source: <http://www.infectioncontroltoday.com/news/2012/07/measuring-the-uncertainties-of-pandemic-influenza.aspx>

Congress OKs plan to combat drug shortages. U.S. House and Senate lawmakers approved a plan to mandate early warnings from drugmakers about possible shortages of crucial medications June 26. The final bill was to reauthorize the Prescription Drug User Fee Act. The legislation reauthorizes for 5 more years Food and Drug Administration (FDA) user fees paid by drug and medical device companies, and it creates new user fees for FDA reviews of generic drugs and biosimilar products. Drugmakers pay the fees in exchange for expedited reviews of new therapies. June 20, the House approved a consensus version of the legislation by voice vote. The Senate followed on June 26 by a vote of 92-4. The U.S. President was expected to sign the measure into law. Drugmakers would be required to notify the FDA at least 6 months before a lifesaving drug is discontinued or if a meaningful, foreseeable disruption in the supply of that drug will occur due to a manufacturing interruption. Source: <http://www.ama-assn.org/amednews/2012/07/02/gvl20702.htm>

FDA clears faster blood test for the market. Listeria, MRSA, Streptococcus, and Enterococcus can all be identified quicker by the Verigene GP Blood Culture Nuclear Acid Test (BC-GP), which got marketing approval from the U.S. Food and Drug Administration (FDA), Food Safety News reported June 28. The Verigene test is manufactured by Northbrook, Illinois-based Nanosphere. FDA's decision was based on the study of 1,642 patient blood samples obtained from incubated blood culture bottles that contained gram-positive bacteria. The study included a comparison of BC-GP and traditional blood culture laboratory methods. The quicker Verigene test was consistent with traditional blood culture methods 93 percent of the time. FDA said BC-GP testing would make it possible to identify potentially serious illness-causing bacteria just hours after a positive blood culture. It is the first nuclear acid test that can identify 12 different bacteria types known to cause bloodstream infections. Traditional tests require 2-4 days to produce bacterial identification and resistance results. The new tests takes just a few hours. Source: <http://www.foodsafetynews.com/2012/06/fda-clears-faster-blood-test-for-the-market/>

(Georgia) Emails reveal security lapses at CDC bioterror laboratory. Internal e-mails revealed repeated, potentially dangerous security lapses at one of the nation's top bio-terror labs that houses deadly biological agents such as anthrax and the SARS virus, ABC News reported June

UNCLASSIFIED

UNCLASSIFIED

28. The e-mails from the Centers for Disease Control (CDC) describe multiple instances between 2009 and 2010 of doors within a supposedly secure facility in Atlanta being left unlocked, potentially allowing unauthorized access to the deadly strains. In at least one instance, someone without the proper security clearance was found in a restricted area. One official said that while walking through a high-security area, he found two doors unlocked and said, "it has become a common failure point," the e-mails said. CDC officials told ABC News the public was never at risk and the agency has addressed the concerns at the Atlanta lab. A CDC spokesperson told USA Today the doors were just one layer of security at the labs and it would still be "close to impossible" for intruders to get their hands on the dangerous microbes. Earlier in June, USA Today reported the same facility was having difficulties with its air flow system, which is designed to keep potentially dangerous air from escaping into "clean" areas. Following the air flow problem reports, Congressional leaders in the House Energy and Commerce Committee launched an investigation into the safety measures at the \$214 million facility. Source: <http://abcnews.go.com/Blotter/emails-reveal-security-lapses-cdc-bioterror-laboratory/story?id=16668649#.T-x8vZfGg-Y>

(Florida) DEA agents raid local pharmacy in statewide investigation. A Drug Enforcement Administration (DEA) pain clinic raid across Florida June 26 landed 14 people in jail. Federal officials deemed the 2 year investigation "Operation Pill Street Blues." Among those cuffed were the owners of Sunset Pharmacy in Fort Myers. Boxes of prescription drugs and logs were seized by DEA agents, but this raid was part of a much bigger bust spanning from Jacksonville to Miami. In all, seven doctors and seven clinic owners were arrested; the seven doctors charged are responsible for dispensing over 2 million Oxycodone tablets. DEA officials said the investigation began in 2010 after reports of a suspicious pain management clinic in Vero Beach. DEA officials said Sunset Pharmacy was responsible for dispensing millions of pills, including Oxycodone, Percocet, Xanax, and Valium, and that doctors were recruited to prescribe these drugs to doctor shoppers, many of whom had patients who were addicts and abused their prescriptions. Source: <http://www.winknews.com/Local-Florida/2012-06-28/DEA-agents-raid-local-pharmacy-in-statewide-investigation>

TRANSPORTATION

(Texas) Drilling trucks have caused an estimated \$2 billion in damage to Texas roads. The new wave of oil and gas production in Texas in recent years has taken a huge toll on the State's roads. The Texas Department of Transportation told industry representatives and elected officials July 2 that repairing roads damaged by drilling activity to bring them up to standard would "conservatively" cost \$1 billion for farm-to-market roads and another \$1 billion for local roads. The estimate does not include the costs of maintaining interstate and State highways. In Johnson County, large producers like Chesapeake Energy and Devon Energy were early to voluntarily cover repairs to roads if presented with before-and-after assessments, a county judge said. However, that was when natural gas prices were high and drilling activity in the Barnett Shale was intense, he said. Now that drilling activity has slowed significantly, the big operators are gone and small subcontractors are hauling salt water and drilling mud, often making it difficult to get anyone to cover road maintenance costs, said a Johnson County

UNCLASSIFIED

UNCLASSIFIED

Precinct 1 commissioner. Six years ago, 90 percent of the roads in his precinct were in good condition. Now, about 60 percent are, he said. Source: <http://www.star-telegram.com/2012/07/02/4075195/drilling-trucks-have-caused-an.html>

(Maryland; Washington, D.C.) Red Line service delayed because of suspicious package. Service on the Red Line was restored between the Fort Totten and Rhode Island Avenue stations in Washington D.C. after being temporarily stopped because of a suspicious package, WJLA 7 Arlington reported June 29. The Metropolitan Police Department reported the suspicious package was in the 4500 block of Fort Totten Drive Northeast. Shuttle bus service ran up between the Rhode Island Avenue, Brookland, and Fort Totten stations during the disruption. Source: <http://www.wjla.com/articles/2012/06/red-line-service-delayed-because-of-suspicious-package-77436.html>

Mexico seeks U.S. intel on airport chief's links to drug trade. The Mexican government asked the United States for information about the alleged links between the director of the Mexico City airport and drug traffickers, Mexico's attorney general said. The director of Mexico City's Benito Juarez International Airport "has links to employees of different drug cartels and facilitates their operations," El Universal newspaper reported June 26, citing U.S. Justice Department documents. Two Mexican federal police officers under investigation for drug trafficking killed three fellow officers who were about to arrest them at the airport June 25. The shooting occurred in the airport's Terminal Two. The two officers were being investigated for their alleged links "to the activities of a drug trafficking network," Mexico's public safety secretary said. The airport director may be called to give a statement as part of the investigation of a network that smuggles drugs through the airport, the attorney general's office sources said. Source: <http://latino.foxnews.com/latino/news/2012/06/27/mexico-seeks-us-intel-on-airport-chief-links-to-drug-trade/>

WATER AND DAMS

High toxic level found in some N.E. wells. A study released the week of June 25 by the U.S. Geological Survey (USGS), found potentially harmful levels of naturally occurring arsenic, uranium, radon, and other contaminants in water supplying wells across the New England region of the United States. Scientists examined water-quality data from 4,800 public-supply wells sampled by the Environmental Protection Agency (EPA) between 1997 and 2007, as well as 117 private wells sampled by USGS from 1995-2007. The samples included only well water from crystalline rock aquifers found in most of New England and small portions of northern New Jersey and southern New York State. The study reported arsenic nearly double the national rate for public drinking water at 13 percent of 2,000 sites tested. Manganese exceeded standards in more than 7 percent, and radon exceeded EPA proposed standards in 33 percent of the wells. They found uranium to be a significant predictor of the presence of other forms of radioactivity that can cause health problems. The health consequences of ingesting water with elevated levels of arsenic, uranium, and other contaminants depends on the concentrations and how long someone drinks the tainted water. Potential issues include various types of cancer, reproductive and developmental problems, kidney and blood diseases, diabetes, and a

UNCLASSIFIED

UNCLASSIFIED

weakened immune system. In addition to natural sources of contamination, human activities have affected the quality of the groundwater from crystalline rock aquifers. Source: http://www.boston.com/news/science/articles/2012/06/28/federal_study_finds_arsenic_and_other_contaminants_pervade_new_englands_groundwater/?page=1

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