

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

Three wildfires scorch parts of western North Dakota. While North Dakota has, for the most part, escaped the large-scale wildfires garnering national headlines and burning the landscapes of neighboring South Dakota and Montana, three fires have caused havoc in the western part of the State. The Bureau of Indian Affairs reported September 21 that the Little Swallow fire had grown to consume 6,000 acres and was just 40 percent contained. Northwest of Dickinson, visitors to Bennett Campground on the Dakota Prairie Grasslands were evacuated after the Trail Side fire broke out. The blaze was about 10 miles northwest of Grassy Butte. Stage I fire restrictions remained in place for the Little Missouri National Grasslands, according to the U.S. Forest Service. Source: <http://www.firehouse.com/news/10783626/three-wildfires-scorch-parts-of-western-north-dakota>

REGIONAL

(Montana) Montana wildfire overview. A Type Two Incident team headed to Lame Deer, Montana, to help fight a wildfire burning south of the town, KULR 8 Billings reported September 25. The Eagle Creek Fire started September 21 and has burned 4,200 acres. The human caused fire is 0 percent contained. Firefighters were making progress on the Wilson Fire, which started the weekend of September 22 near Roundup. Officials with Musselshell County said that the fire is at 100 percent containment, and is estimated to have burned 3,600 acres of land southeast of Roundup. Residents east of U.S. Highway 83 in the Condon area were asked to prepare for possible evacuation as a lightning-caused fire moves closer to homes. The Condon Mountain Fire burned 4,450 acres since it started July 28. September 25, the fire was burning within 1.5 miles of a dozen residences about 4 miles northeast of Condon in the Swan Valley. The U.S. Forest Service said the fire is burning in steep, hazardous terrain with heavy timber with numerous standing snags east of the Bob Marshall Wilderness. The Flathead National Forest has closed the area around the fire for public safety. A temporary flight restriction was in effect surrounding the Condon Mountain Fire area, and the Condon Airport was closed to all non-fire aircraft until further notice. Source: <http://www.kulr8.com/news/local/Montana-Fire-Overview-171190051.html>

(Montana) Drought continues with 13 new counties declared natural disaster areas. With weeks of little to no rain, more than 60 percent of Montana was experiencing some severity of drought conditions, according to the National Oceanic and Atmospheric Administration (NOAA). September 20, NOAA released its' weekly Drought Monitor, which showed no improvement for the State. As the dry weather persists, the U.S. Department of Agriculture Farm Service Agency (USDA FSA) declared 13 new counties as primary natural disaster areas. This designation allows farm operators to apply for low interest emergency loans from the USDA FSA. Those counties include Carbon, Carter, Cascade, Golden Valley, Judith Basin, Meagher, Musselshell, Park, Powder River, Stillwater, Sweet Grass, Treasure, and Wheatland. Nearby counties are also eligible for natural disaster assistance. Those include Big Horn, Broadwater, Chouteau, Custer, Fallon, Fergus, Gallatin, Lewis and Clark, Petroleum, Rosebud, Teton, and Yellowstone. Source:

UNCLASSIFIED

<http://www.krtv.com/news/drought-continues-with-13-new-counties-declared-natural-disaster-areas/>

NATIONAL

Nothing Significant to Report

INTERNATIONAL

Moldova says it detains uranium dealers from rebel region. Moldovan police detained seven suspected members of a group that traded firearms and uranium-235, operating in the separatist Transdniestria region, the country's interior ministry said September 21. —We have documented numerous cases involving shipments of hand grenades, TNT blocks, Kalashnikov assault rifles, rocket-propelled grenade (RPG) launcher charges, and containers with radioactive uranium-235, the head of the ministry's investigations department told reporters. Source: http://articles.chicagotribune.com/2012-09-21/news/sns-rt-us-moldova-uraniumbre88k0x1-20120921_1_uranium-detains-moldovan

3 killed in inmate hunt shootout near US border. Authorities in Mexico said three gunmen have been killed after attacking police hunting for inmates who joined in a mass escape from a prison near the U.S. border. The Coahuila state prosecutor's office said the gunmen were in a truck in a residential area of the border city of Piedras Negras when they fired on state police officers September 20 who were helping look for some of the 131 prisoners who fled a nearby prison earlier the week of September 17. Investigators have yet to determine whether the dead gunmen were escapees. The statement said the truck matches records of a vehicle stolen in San Antonio. Authorities said the Zetas drug cartel orchestrated the prison break apparently with the help of prison personnel. Three escapees have been recaptured so far. Source: http://www.wtnh.com/dpp/news/international/3-killed-in-inmate-hunt-shootout-near-US-border_25957422

BANKING AND FINANCE INDUSTRY

Hackers strike U.S. Bank with volunteer-powered DDoS. U.S. Bank's Web site was disrupted September 26 in a people-powered distributed denial of service (DDoS) attack, launched by a group of hackers who have claimed responsibility for similar cyberattacks against four other banks in the United States, CSO Online reported September 27. The attack involved hundreds of thousands of computers sending an overwhelming number of requests that downed the site for roughly an hour, according to a security researcher at FireEye. The disruption of U.S. Bank's Web site came 1 day after a similar attack against Wells Fargo & Co. The group has taken credit for other attacks that occurred the week of September 17, against Bank of America, JPMorgan Chase, and Citigroup. A representative of U.S. Bancorp, which operates as U.S. Bank, confirmed it was under attack and experiencing disruptions. Rather than launch the attack from a network of compromised machines, called a botnet, the attackers are apparently using volunteers, the FireEye researcher said. Participants go to either one of two file-sharing sites and download a

UNCLASSIFIED

UNCLASSIFIED

program written in a scripting language. Once the program is running, a person only has to click on a —start attack button to send continuous requests to the target's Web site. This method makes it more difficult for authorities to stop the attack, because there are no control servers. The group had said on a Pastebin post that it would attack Wells Fargo September 25, U.S. Bank September 26, and PNC Financial Services Group September 27. Source:

<http://www.pcadvisor.co.uk/news/security/3400907/hacktivists-strike-us-bank-with-volunteer-powered-ddos/>

Wells Fargo recovers after site outage. Wells Fargo's Web site experienced intermittent outages September 25, while the hacker group claiming responsibility threatened to hit U.S. Bancorp and PNC Financial Services Group over the next 2 days, IDG News Service reported. Wells Fargo apologized on Twitter for the disruption, and said they were working to restore access. By September 26, the site appeared to be functioning. A group calling itself the —Mrt. Izz ad-Din al-Qassam Cyber Fighters said it coordinated the attacks, and planned further ones on U.S. Bancorp September 26 and PNC Financial Services Group September 27, according to a post on Pastebin. The group said the cyberattacks are in retaliation for the 14-minute video trailer insulting the Prophet Muhammad, and said the attacks will continue until the video is removed from the Internet. The attacks would last 8 hours starting at 2:30 p.m. GMT, the group wrote. Source:

http://www.computerworld.com/s/article/9231721/Wells_Fargo_recovers_after_site_outage

Stolen card data on sale on professional-looking e-shop. A researcher from Webroot recently uncovered a seemingly well-established Web site for selling stolen card data, so much so that the crook behind the scheme has set up a professional-looking e-shop. The shop is advertised on a number of carding forums, and the crook can be contacted only via ICQ. The page is well designed and features a shop whose functionality does not seem to differ much from any other legitimate one. The e-shop also has a helpful search engine so customers can find exactly what they need. —The service is currently offering 9,132 stolen credit cards for sale, and has already managed to sell 3,292 credit cards to prospective cybercriminals, the researcher said, noting that the going rate for a sample stolen credit card depends on whether the card is debit or credit. The former go for \$16, and the latter for \$30 per item, but there are also discounts to be had for bulk purchases. Rather than exploiting the stolen card numbers, services like the e-shop forward the risk on to those who purchase the numbers and then attempt to exploit them.

Source: <http://www.net-security.org/secworld.php?id=13652>

Bank of America website reveals details of random users, experts find. While logging in to Bank of America's (BoA) Web site to access the Automated Clearing House (ACH) system, experts from Private Internet Access noticed they were actually viewing the bank account details of some other random customer, Softpedia reported September 25. After they entered the transfer interface, they were presented with the name, bank account, balance, email address, and other details of an individual who had nothing to do with the company. Apparently, the account is restored to normal after the user logs out and logs back in again, and the security hole could not be reproduced after this first occurrence. However, some users reported that they also encountered the problem in the past, which meant that it was not an

UNCLASSIFIED

UNCLASSIFIED

isolated incident. Private Internet Access representatives made screenshots and sent out a detailed notification to BoA. Source: <http://news.softpedia.com/news/Bank-of-America-Website-Reveals-Details-of-Random-Users-Experts-Find-294534.shtml>

U.S. regulators concerned about Vegas bets on Chinese VIPs. U.S. regulators are worried about a Macau-based foreign tour industry they say exposes Las Vegas to money laundering, the Wall Street Journal reported September 20. The paper reported how some Chinese high-roller gamblers use —junkets, as foreign-tour operators are known, to get around a requirement that Chinese residents only take \$50,000 in currency abroad a year. U.S. casinos are increasing their bets on the business, much to the concern of regulators worried that junket operators are bringing new money laundering methods to Las Vegas. The U.S. Treasury Department’s Financial Crime Enforcement Network (FinCEN) issued a Web alert in August to casinos advising them to monitor junket operations and junket patrons and report —all available information on any suspicious activity. Some junket industry activity on FinCEN’s radar includes obscuring the source of their funding, the method for transferring it to high rollers, and the identities of the gamblers themselves. Source: <http://blogs.wsj.com/corruption-currents/2012/09/20/u-s-regulators-concerned-about-vegas-bets-on-chinese-vips/>

Justice Dept to highlight investment fraud scams. With investment fraud cases piling up in the weak economy, the U.S. Justice Department (DOJ) is holding summits around the country to warn investors about the scams, which are often carried out by people with personal ties to the victims, the Associated Press reported September 23. The first regional conference is set for October 1 in Connecticut, where federal prosecutors have announced several fraud cases in September, including that of a man who cheated clients from his church. Summits are also planned for later October in Cleveland, Nashville, Miami, Denver, and San Francisco. Nationwide, federal prosecutors looking at investment cases from the last 2 years identified 500 prosecutions that targeted 800 defendants and involved more than \$20 billion in fraud, a U.S. attorney said. The northeastern summit, hosted by the DOJ as well as the Securities and Exchange Commission, will bring together officials from agencies including the FBI as well as top federal prosecutors from neighboring States at the Stamford campus of the University of Connecticut. Topics to be addressed include case studies and the perspective of fraud victims. Source:

http://www.google.com/hostednews/ap/article/ALeqM5iQyVrPqzBZyH7yA_CrUc_FTXcg5A?docId=33e7e50f1f8145d5aba40fcc17d43880

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

23 nuclear plants in tsunami risk zones. A recent study led by European researchers found 23 nuclear power plants around the world may be susceptible to destructive tsunami waves, with most of them in east and southeast regions of Asia, LiveScience reported September 24. The 23 facilities on the list (including the Fukushima plant) house a total of 74 nuclear reactors. Thirteen of the plants are active, while the others are either nearing completion or being expanded to house more reactors. The study, which appears in a recent issue of the journal Natural Hazards, urges energy officials in potentially affected countries to consider how they

UNCLASSIFIED

UNCLASSIFIED

would deal with the potential consequences of a tsunami impacting a nuclear power plant.

Source: <http://news.discovery.com/earth/nuclear-plants-at-tsunami-risk-120924.html>

Environmental Protection Agency announces changes to chemical assessment program. In a major change to its chemicals assessment program, the U.S. Environmental Protection Agency (EPA) will seek early input about chemicals under review, Chemical & Engineering News reported September 24. Stakeholders from industry and others will be able to provide their views about a substance's toxicity before EPA decides what data to rely on for the assessments, according to the agency. The director of the EPA's National Center for Environmental Assessment announced the change the week of September 17 before a new National Research Council committee. The council is reviewing the agency's chemical hazard assessment database — called the Integrated Risk Information System (IRIS) — for Congress. EPA's IRIS assessments provide scientifically-based judgments on the safe dose of a chemical, which is the maximum exposure to the substance that will not cause health effects. EPA, other federal and State agencies, and some foreign countries, use IRIS to guide regulation. Source:

<http://cen.acs.org/articles/90/i39/Environmental-Protection-Agency-Announces-Changes.html>

COMMERCIAL FACILITIES

(Florida) Police: Shoplifter kills Wal-Mart security employee, then self. A suspect who tried to steal undershirts valued at \$16 from a Wal-Mart in Margate, Florida, shot and killed a loss prevention employee there September 21, police said. The victim was pronounced dead at a local hospital after the shooting, a Margate police spokesman said. The suspect fled on foot, and police said they later found what they believed to be the suspect's body, which appeared to have a self-inflicted gunshot wound. A woman was also taken into custody but her involvement in the incident was unknown. After the shooting, police from Sunrise, Margate, Coconut Creek, and Plantation converged on the scene, and a helicopter flew in the area searching for the suspect. Source: <http://usnews.nbcnews.com/news/2012/09/22/14033160-police-shoplifter-kills-wal-mart-security-employee-then-self?lite>

(Michigan) Meth lab closes downtown Lansing business. Materials such as tubing and bottles... were just some of the meth-cooking materials found in the kitchen area of a break room in the Insurance Institute of Michigan offices in Lansing, Michigan, September 19. A police spokesman said officials hoped to get details from the two suspects in custody at the city jail. The suspects found by police with the meth-making materials are janitors who were working their weekly, after-hours shift at the institute. It is a business leasing a portion of the Michigan Beer and Wine Wholesalers Association building. It was a portable operation, something police call one-pot meth making, where as long as one has all of the proper materials, the drug can be made almost anywhere in 20-30 minutes. The executive director of the insurance institute, and his employees now have to work from home indefinitely. He is waiting for the health department to make sure there are no leftover fumes or material that could harm anyone. Source: <http://www.wilx.com/news/headlines/Meth-Lab-Closes-Downtown-Lansing-Business-170576496.html>

UNCLASSIFIED

UNCLASSIFIED

COMMUNICATIONS SECTOR

Sprint says Virgin Mobile users are safe from account hijacks. Sprint September 19 denied that subscribers of its Virgin Mobile subsidiary were wide open to account hijacking attacks as claimed by an independent software developer the week of September 17. In emailed comments, a Sprint spokeswoman said the company has multiple safeguards to protect customer accounts from intrusion and tampering by unauthorized users. She was responding to questions that arose from a September 17 blog post by a developer. In it, he detailed how the username and password system used by Virgin Mobile to let users access their accounts online was inherently weak and open to abuse. Virgin forces subscribers to use their phone numbers as their username and a six-digit number as their password, he noted. The developer said he went public with his discovery because Sprint did not fix the vulnerability after being told how easy it was to exploit. He also noted in his blog that Virgin Mobile subscribers had no easy way to mitigate any exposure to account hijacks. In response, Sprint said it implemented a new procedure to lock out users from their accounts after four failed attempts. The developer described that move as ineffective because hackers could bypass it by making log-in attempts without sending any cookie data with the requests. Source:

http://www.computerworld.com/s/article/9231470/Sprint_says_Virgin_Mobile_users_are_safe_from_account_hijacks

CRITICAL MANUFACTURING

NHTSA recall notice - Triumph Daytona 675 and Street Triple regulator/rectifier overheating. Triumph announced September 24 the recall of 10,366 model year 2006-2009 Street Triple, Street Triple R, and Daytona 675 motorcycles. The regulator/rectifier can overheat and prevent the motorcycle from charging. Once the battery is fully discharged, the motorcycle may stall. If the motorcycle stalls, there is an increased risk of a crash leading to personal injury. Triumph will notify owners, and dealers will inspect and replace the regulator/rectifier. Source:

http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcld_ID=12V445000&summary=true&prod_id=396690&PrintVersion=YES

GM recalling almost 474,000 cars over problem with gear shift. General Motors Co (GM) announced September 21 the recall of 473,841 model year 2007-2010 Chevrolet Malibu, Pontiac G6, and Saturn Aura vehicles globally to fix a condition that could lead the cars to roll when the drivers think they are in park. GM said it was aware of four crashes that resulted from the problem, but no injuries. The company said the recall affected vehicles equipped with four-speed automatic transmissions. GM will repair the condition in which the transmission gear position may not match the gear on the shifter. Dealers will reinforce the shift cable end fitting to prevent that part from fracturing, GM said. Owners will be notified by letter to schedule the free repairs at dealers, and those who have had the work done already will be eligible for reimbursement. Source: <http://bottomline.nbcnews.com/news/2012/09/21/14009262-gm-recalling-almost-474000-cars-over-problem-with-gear-shift?lite>

UNCLASSIFIED

DEFENSE/ INDUSTRY BASE SECTOR

Keeping nukes safe from cyber attack. In the wake of a 2010 incident in which the U.S. Air Force lost contact with 50 intercontinental ballistic missiles (ICBMs), the service is figuring out how to protect its command-and-control systems from cyberattack, Foreign Policy reported September 25. Global Strike Command manages U.S. land-based nuclear ICBMs and air-launched nuclear cruise missiles and bombs. The need to protect these military assets from cyberattack and avoiding the scenario of an enemy feeding incorrect information into the nuclear command-and-control networks seized Air Force officials after they lost contact with a field of 50 Minuteman III ICBMs at FE Warren Air Force Base in Wyoming for an hour in late 2010. —There was an issue: we had a temporary interruption in our ability to monitor one of our missile squadrons back in the fall of 2010. That produced a need to take a comprehensive look at the entire system. It took a year to do that study, and we're confident that the system is good, but as we upgrade it, modernize it, integrate it, we've got to really pay attention to protecting nuclear command-and-control information, according to the head of Air Force Global Strike Command's nuclear deterrence division. He said they are working to harden their networks against intrusion and the manipulation of nuclear command-and-control information and to increase backup communications abilities. —We are continuing to study the cyber assurance aspect of the supply chain that supports our nuclear weapons systems, he also said. Source:

http://killerapps.foreignpolicy.com/posts/2012/09/25/keeping_nukes_safe_from_cyber_attack

(New Jersey) Jury convicts man for taking military tech info. A former employee of a New Jersey-based defense contractor was found guilty September 26 of taking U.S. military technology trade secrets from his employer and exporting them to his native China. He worked for Space & Navigation, a New Jersey division of New York-based L3 Communications. The man, who lived until recently in Flanders, New Jersey, was arrested at his home in Deerfield, Illinois, in March 2011 and accused of taking restricted military data and presenting them at two conferences in China during the fall of 2010. Prosecutors argued the technology was proprietary and could be used for target locators and other military applications. A federal jury in Newark, New Jersey, found the man guilty on nine counts, including exporting defense-related data without a license, possessing stolen trade secrets, and lying to federal agents. He was acquitted on two counts of lying to federal authorities about one of his visits to China.

Source: <http://www.militarytimes.com/news/2012/09/ap-jury-convicts-man-military-tech-information-092612/>

(Oregon) Defense contractor employee aids phony parts probe. Court records made public September 25 show that a new search of an Oregon defense contractor accused of providing phony helicopter and truck parts to the military was prompted by testimony from a purchasing agent who is helping investigators. An affidavit filed in court in Eugene says investigators went looking at Kustom Products Inc. in Coos Bay the week of September 17 for purchase orders and sample parts used as prototypes for phony parts. A DHS special agent wrote the search was prompted by three interviews in the past 2 months with the company's former purchasing agent, who faces federal charges along with the company's owner and several members of his

UNCLASSIFIED

family. The indictment alleges they supplied counterfeit parts to the military in hundreds of contracts totaling \$7.5 million. Authorities are also asking a judge to authorize seizure of profits and goods such as pickup trucks and boats bought with profits. Trial is set for January 26, 2013. The investigation was triggered when Kentucky Army National Guard mechanics noticed replacement lock nuts for the rotor assembly of Kiowa attack helicopters did not meet specifications. They said failure of the nuts could cause helicopters to crash. Source: <http://www.manufacturing.net/news/2012/09/defense-contractor-employee-aids-phony-parts-probe>

Another IE exploit targeting defense industry discovered. Another malicious Web site was discovered hosting an exploit for the zero-day vulnerability Internet Explorer patched by Microsoft the week of September 17. This site, like the other exploits discovered, targets the defense and space industries, and is dropping an unknown payload, according to Barracuda Labs. One researcher said the compromised site is not likely a drive-by attack, but instead may be included in phishing email messages to specific individuals within those respective industries. Previous exploits were dropping either the Poison Ivy or PlugX remote access trojans. This malicious file discovered by Barracuda has a similar file name to the others, Grumgog.swf, named after a character in a video game. Barracuda did not identify the payload dropped here, but did call it a backdoor. Source: http://threatpost.com/en_us/blogs/another-ie-exploit-targeting-defense-industry-discovered-092412

EMERGENCY SERVICES

(Colorado) 1 staffer killed, another injured in Colo. prison. A female kitchen employee was killed and another seriously injured September 24 in a disturbance involving an inmate while breakfast was being prepared at Arkansas Valley Correctional Facility in Crowley, Colorado, a spokeswoman said. State investigators were called to the prison to try to determine what happened. Meals were being delivered from other facilities after the kitchen was shut down, and the prison was placed on lockdown. Source: <http://www.wect.com/story/19622431/2-staffers-injured-in-sw-colo-prison-disturbance>

ENERGY

Study: States fail to enforce Marcellus Shale drilling regulations. September 25, Earthworks, a nonprofit, released Breaking All the Rules: The Crisis in Oil & Gas Regulatory Enforcement, a new research study indicating that States across the country — including Pennsylvania — are failing to enforce their own oil and gas development regulations. The 1-year, in-depth research project examined enforcement data and practices in Pennsylvania, Texas, Ohio, New York, New Mexico, and Colorado and included interviews with ex-industry and State agency employees. Failure to enforce oil and gas regulations means that States are not seeking, documenting, sanctioning, deterring, and cleaning up problems associated with irresponsible oil and gas operations such as chemical spills, equipment failure, accidents, and discharges into drinking water supplies, the report stated. Source: <http://canon-mcmillan.patch.com/articles/study-states-fail-to-enforce-marcellus-shale-drilling-regulations>

UNCLASSIFIED

UNCLASSIFIED

FERC creates new cybersecurity division in bid to secure critical infrastructure. Officials at the Federal Energy Regulatory Commission (FERC) September 20 announced the creation of the agency's new Office of Energy Infrastructure Security (OEIS), which will work to reduce threats to the electric grid and other energy facilities, Federal Computer Week reported September 21. The goal is for the office to help FERC, as well as other agencies and private companies, better identify potential dangers and solutions. According to FERC, the OEIS will focus on developing recommendations for identifying, communicating and mitigating cyber and physical threats and vulnerabilities; providing assistance and expertise to other government organizations; participating in collaborative, interagency efforts; and conducting outreach to the private sector. Source: <http://fcw.com/articles/2012/09/21/ferc-new-critical-infrastructure-cybersecurity-office.aspx>

Dell SecureWorks uncovers cyber espionage targeting energy firms. Dell SecureWorks researchers discovered a cyber espionage campaign targeting several large companies, including two in the energy sector, ComputerWeekly.com reported September 20. The campaign, dubbed Mirage, targeted an oil company in the Philippines, an energy firm in Canada, a military organization in Taiwan and other unidentified targets in Brazil, Israel, Egypt, and Nigeria. This is the second cyber espionage campaign to be uncovered during 2012 by the Counter Threat Unit of security firm Dell SecureWorks. The first campaign, dubbed Sin Digoo, targeted several petroleum companies in Vietnam, government ministries in different countries, an embassy, a nuclear safety agency, and other business related groups. The Dell SecureWorks researchers believe either the same group is behind both campaigns, or whoever is responsible for Mirage is working closely with those behind Sin Digoo. Source: <http://www.computerweekly.com/news/2240163620/Dell-SecureWorks-uncovers-cyber-espionage-targeting-energy-firms>

Flawed ORing networking devices expose oil and gas companies to cyberattacks. DHS' Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory to warn customers of ORing Industrial Networking devices of a serious vulnerability that exposes their organizations to cyberattacks, Softpedia reported September 21. A remote attacker who knows the hard-coded credentials can exploit the affected product by logging into the device with administrative privileges. This gives him/her permission to change the system's settings, and even read and write files. —An attacker can log into the operating system of the device using an SSH connection with the root credentials to gain administrative access. Once the attacker gains access to the device, the file system and settings can be accessed, which could result in a loss of availability, integrity and confidentiality, ICS-CERT reports. The products susceptible to such attacks are industrial serial device servers and they are used for SCADA systems. Source: <http://news.softpedia.com/news/Flawed-ORing-Networking-Devices-Expose-Oil-and-Gas-Companies-to-Cyberattacks-293994.shtml>

UNCLASSIFIED

FOOD AND AGRICULTURE

FSIS issues new Salmonella guide for small entities. The Food Safety and Inspection Service (FSIS) issued a revised compliance guide that will help small and very small meat and poultry establishments produce ready-to-eat products with respect to Salmonella and other pathogens, Occupational Health & Safety reported September 21. Posted September 19, the guide is not available in hard copy, according to the FSIS notice announcing its availability. Source: <http://ohsonline.com/articles/2012/09/21/fsis-issues-new-salmonella-guide-for-small-entities.aspx?admgarea=ht.FoodSafety>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

GAO: Easily obtained counterfeit IDs present real risks. The Government Accountability Office (GAO) released a report September 21 in which the agency demonstrates that counterfeit documents can still be used easily to obtain valid driver's licenses and State-issued identification cards under fictitious identities. GAO recommended that DHS exert more assertive leadership in an effort to correct the problem, Homeland Security News Wire reported September 26. The president of the Coalition for a Secure Driver's License, stated, —The GAO replicated the same techniques used by the 9/11 terrorists to get more than 30 driver's license and IDs from State licensing agencies. To obtain a driver's license with your photo but with someone else's biographic information or with fictitious information, terrorists need only travel to a State where identification standards are low and service is fast. Terrorists planning future attacks on Americans will be delighted by GAO's findings, but Congress should be very concerned. A coalition release notes that GAO's investigators obtained five driver's licenses in three different States under fictitious identities using combinations of name, birth date, and Social Security numbers together with counterfeit documents. In two States, a GAO investigator was able to obtain two licenses with different identities using the same person's face. Only in one case did a motor vehicle employee appear to question the validity of the documents being presented, but the GAO investigator was still able to obtain a driver's license. Source: <http://www.homelandsecuritynewswire.com/dr20120926-gao-easily-obtained-counterfeit-ids-present-real-risks>

(Pennsylvania) Western Pa. community college reopens day after threat to release nerve chemical on campus. Westmoreland County Community College (WCCC) in Youngwood, Pennsylvania, reopened its campuses a day after receiving threatening phone calls. WCCC officials confirmed the school had reopened September 25. State police from nearby Greensburg were also investigating. County emergency officials said the caller had threatened to release an explosive nerve chemical unless some kind of ransom was paid by 4 p.m. September 24. No dangerous incidents had been reported, however. Source: <http://www.therepublic.com/view/story/5efe541b4b7341e29aad706dee670e07/PA--Community-College-Threat>

UNCLASSIFIED

US Department of Agriculture sites hacked in protest against Mohammed movie. Hackers from the Bangladesh Cyber Army protested against the Innocence of Muslims video by breaching three subdomains owned by the U.S. Department of Agriculture. —We are BANGLADESH CYBER ARMY, the first and largest hacking group of Bangladesh! Recently, a movie was released where the Prophet of Islam, Hazrat Muhammad (Sm) was insulted, the hackers told Softpedia in an email. —There was a protest regarding removal of the movie. Being a cyber army of the Muslim world, we felt necessary to join the protest. As a result, we hacked a few of US Government sites. A number of normal US sites were also hacked. Source: <http://news.softpedia.com/news/US-Department-of-Agriculture-Sites-Hacked-in-Protest-Against-Mohammed-Movie-293926.shtml>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Espionage hackers target ‘watering hole’ sites. Security experts are accustomed to direct attacks, but some of today’s more insidious incursions succeed in a roundabout way — by planting malware at sites deemed most likely to be visited by the targets of interest. New research suggests these so-called —watering hole tactics have recently been used as stepping stones to conduct espionage attacks against a host of targets across a variety of industries, including the defense, government, academia, financial services, healthcare, and utilities sectors. In a report released September 25, RSA FirstWatch’s (RSA) experts hint at — but do not explicitly name — some of the watering hole sites. According to RSA, the sites in question were hacked between June and July 2012. Source: <http://krebsonsecurity.com/2012/09/espionage-hackers-target-watering-hole-sites/>

Rent-to-own laptops were spying on users. The U.S. Federal Trade Commission (FTC) settled a case with several computer rent-to-own companies and a software maker over their use of a program that spied on as many as 420,000 users of the computers. The terms of the settlement will ban the firms from using monitoring software, deceiving customers into giving up information, or using geo-location to track users. The software for rental companies from DesignerWare included a —Detective Mode, a spyware application that, according to the FTC’s complaint, could activate the Webcam of a laptop and take pictures and log keystrokes of user activity. The software also regularly presented a fake registration screen designed to trick users into entering personal information. The data collected was transmitted to DesignerWare and then passed on to the rent-to-own companies. DesignerWare sold the service, which included a —kill switch to disable the machine, to be activated if a computer was stolen or a renter was late making payments. However, the data gathered also contained user names and passwords for email accounts, social media Web sites, and financial institutions, said the FTC. The complaint said Social Security numbers, private email with doctors, bank and credit card statements, and Webcam pictures of —children, partially undressed individuals and intimate activities at home were collected. The complaint against DesignerWare said its licensing and enabling of —Detective Mode was providing the rent-to-own companies with the means to break the law. Source: <http://www.h-online.com/security/news/item/Rent-to-own-laptops-were-spying-on-users-1717567.html>

UNCLASSIFIED

UNCLASSIFIED

Most data breaches come from within. While the data breach events that catch headlines are the work of hacking collectives and professional malware writers, it turns out that the vast majority of information compromises are caused by companies' own unwitting employees. According to new research from Forrester, only 25 percent of data breach cases are the work of external attackers, and only 12 percent of them were perpetrated by insiders with ill intent. That leaves 63 percent of the issues caused by something more mundane, like losing or misplacing corporate assets, the report found. Source: <http://www.infosecurity-magazine.com/view/28404/most-data-breaches-come-from-within/>

A single Web link will wipe Samsung Android smartphones. A hacker demonstrated how a simple Web page can reset various Samsung phones back to the state they left the factory — enabling a click, bump, or text to take out a victim's mobile device entirely. The flaw lies in Samsung's dialing software, triggered by the tel protocol in a URL. It is not applicable to all the company's Android handsets, but those that are vulnerable can have their PIN changed or be wiped completely just by visiting a Web page or snapping a bad QR code, or even bumping up against the wrong wireless NFC tag. Source: http://www.theregister.co.uk/2012/09/25/samsung_flaw/

One billion users affected by Java security sandbox bypass vulnerability, experts say.

Researchers from Security Explorations claimed to identify a flaw that affects all Oracle Java SE versions and the billions of devices on which the software is currently installed. This bug, codenamed issue 50, was identified just before the start of Oracle's JavaOne 2012 conference. —The impact of this issue is critical — we were able to successfully exploit it and achieve a complete Java security sandbox bypass in the environment of Java SE 5, 6 and 7, the CEO of Security Explorations said. He said the vulnerability can be leveraged by an attacker to —violate a fundamental security constraint of Java Virtual Machines. The researchers confirmed Java SE 5 — Update 22, Java SE 6 — Update 35, and Java SE 7 Update 7 running on fully patched Windows 7 32-bit operating systems are susceptible to the attack. The affected Web browsers are Safari 5.1.7, Opera 12.02, Chrome 21.0.1180.89, Firefox 15.0.1, and Internet Explorer 9.0.8112.16421. The company provided Oracle with a complete technical description of the flaw, along with source and binary codes, and a proof-of-concept that demonstrates the complete security sandbox bypass in Java SE 5, 6, and 7. Source: <http://news.softpedia.com/news/One-Billion-Users-Affected-by-Java-Security-Sandbox-Bypass-Vulnerability-Experts-Say-294629.shtml>

DHL: Most common word used in spear phishing attacks in 2012 H1. In a new report, FireEye identified a trend in the words being utilized in the names of malicious files sent in spam campaigns. In the second half of 2011, the most common word used in such cybercriminal campaigns was —label. In the first half of 2012, —label dropped to the 6th position. Currently, the most commonly utilized words in spear phishing attacks are —dhl and —notification. Each of these words appears in almost a quarter (23.42 percent and 23.37 percent, respectively) of all the malicious attachments that land in users' inboxes. Other words that stand out are —delivery, —express, —2012, —shipment, —ups, —international, —parcel, —post, —confirmation, —alert, —usps, —report, —jan2012, —april,

UNCLASSIFIED

UNCLASSIFIED

—idnotification, —ticket, and —shipping. This shows that most of the malicious files that come via spam emails are somehow related to shipping. While this may not seem new, the figures from the report reveal that names related to this topic have grown from 19.20 percent to 26.35 percent. Source: <http://news.softpedia.com/news/DHL-Most-Common-Word-Used-in-Spear-Phishing-Attacks-in-2012-H1-294570.shtml>

Hactivism skews security trend analysis. The re-emergence of the hacktivist movement appears to have caused complications for those in the information security industry charged with data breach trend analysis. There has been a series of massive data breaches over the last 16 months — each of which compromised more than 1 million identities. During the same time, much smaller incidents occurred in which only a handful of records were stolen. CQR Consulting’s chief technology officer said in July that the Anonymous hacking collective —tend[ed] to find the vulnerable sites first, and justify their actions afterwards. The Symantec’s August Intelligence Report reflected the skewed results in a comparison of the first 8 months of 2012 against the last 8 months of 2011, covering what the company said was the revival of the hacktivist AntiSec (anti-security) campaign. Source: <http://www.scmagazine.com.au/News/316698,hactivism-skews-security-trend-analysis.aspx>

Stuxnet tricks copied by computer criminals. Experts indicate the techniques used in sophisticated, state-backed malware are trickling down to less-skilled programmers who target regular Web users and their online accounts or credit card details. State-sponsored malware became widely known in 2010 with the discovery of Stuxnet, a program targeted at Iranian industrial control systems. Since then, several other very sophisticated malware packages have been discovered that are also believed to have been made by governments or government contractors. These packages include Duqu, exposed late in 2011, and Flame, found in May 2012. One reason such malware is so effective is it tends to exploit previously unknown software vulnerabilities, known as zero-days, in widely used programs such as Microsoft Windows to gain control of a computer. A Kaspersky researcher said those exploits can be quickly —copy-pasted by other programmers, as happened after the discovery of Stuxnet. More concerning is the way higher-level design features are being picked up, he said. Source: <http://www.technologyreview.com/news/429173/stuxnet-tricks-copied-by-computer-criminals/>

Energy lab develops Sophia to help secure SCADA systems. New cybersecurity software developed by an Energy Department lab specifically for utilities and other industrial systems could be available as early as October. The Idaho National Laboratory’s Sophia software sentry, funded by the Energy Department’s Office of Electricity Delivery & Energy Reliability and DHS, passively monitors networks to help operators detect intruders and other anomalies. Industrial systems such as power plants have concentrated on physical security because they were not connected to the Internet, but that has changed as operators have added computer networks. Sophia is a tool to automate real-time monitoring on static Supervisory Control and Data Acquisition (SCADA) system networks — those with fairly fixed communications patterns. Anything out of the ordinary triggers an alert. If the program detects suspicious activity, it alerts an operator or network administrator, who can then decide if the activity is threatening.

UNCLASSIFIED

UNCLASSIFIED

Source: <http://gcn.com/articles/2012/09/20/inl-sophia-industrial-control-system-security-tool.aspx>

IBM: Top threats include data breaches, BYOD, browser exploits. When it comes to trends in security for 2012 so far, the landscape has seen a sharp increase in browser-related exploits, like recent ones for Internet Explorer and Java, along with renewed concerns around social media password security and continued disparity in mobile devices and corporate bring-your-own-device (BYOD) programs. That information comes from the IBM X-Force 2012 Mid-Year Trend and Risk Report, which shows that a continuing trend for attackers is to target individuals by directing them to a trusted URL or site injected with malicious code. Through browser vulnerabilities, the attackers are able to install malware on the target system. Further, the growth of SQL injection, a technique used by attackers to access a database through a Web site, is keeping pace with the increased usage of cross-site scripting and directory traversal commands. Source: <http://www.infosecurity-magazine.com/view/28370/ibm-top-threats-include-data-breaches-byod-browser-exploits>

NATIONAL MONUMENTS AND ICONS

(California) Workers could be tested for hantavirus. California public health officials want to survey workers at Yosemite National Park to determine whether they were exposed to a deadly mouse-borne virus, a park spokesman said September 20. The California Department of Public Health recently proposed to take a voluntary survey of workers to contribute to the park's understanding of hantavirus and the recent disease cluster, a Yosemite National Park spokesman said. The Mariposa Gazette reported September 20 that three park workers experienced flu-like symptoms and got tested for hantavirus. A Mariposa County Health Officer told the Mariposa County Board of Supervisors at a September 18 meeting that while initial tests came up positive, a second set of tests showed the workers were not exposed to the strain that causes hantavirus pulmonary syndrome. The Yosemite National Park spokesman said there have been no confirmed or suspected cases among employees of the National Park Service or the park's concessionaire, DNC Parks and Resort. Nine people who spent time at the park this summer have been infected with the rodent-borne virus, the majority after staying at the —Signature cabins in Curry Village. Three of them have died. Source: http://www.mercurynews.com/breaking-news/ci_21598139/workers-could-be-tested-hantavirus

POSTAL AND SHIPPING

(California) Bomb scare at Lone Pine Post Office. There was a bomb scare in Lone Pine, California, September 14 at the town's post office, the Inyo Register reported September 20. The incident ended with the discovery of what was described as —bizarre writing and ramblings stuffed inside two —cylindrical containers, a sheriff's department public information officer said. The containers themselves were covered with writings and swastikas, and were left on the sidewalk outside of the Lone Pine Post Office at an unknown time. Employees found the containers, and after 45 minutes reported the packages as suspicious.

UNCLASSIFIED

UNCLASSIFIED

Fearing the containers could contain explosives, law enforcement implemented evacuation procedures and requested the response of the sheriff's department's explosives expert. The sheriff's department evacuated businesses within a 1-mile radius of the post office. The containers were ultimately removed from the scene and taken to a remote, undisclosed location and detonated. Inside the containers were more —bizarre writings and ramblings, officials said. The incident was under investigation. Source:

<http://www.inyoregister.com/node/3581>

PUBLIC HEALTH

U.S. warns hospitals on Medicare billing. Saying there were —troubling indications of abuse in the way hospitals use electronic records to bill for Medicare and Medicaid reimbursement, the Presidential administration warned September 24 it would vigorously prosecute doctors and hospitals implicated in fraud. The Secretary of Health and Human Services and the Attorney General said in a letter sent to five major hospital trade associations that the government would not tolerate attempts to —game the system. The strongly worded letter said —there are troubling indications that some providers are using this technology to game the system, possibly to obtain payments to which they are not entitled. The letter cited possible abuses including —cloning of medical records, where data about one patient was repeated in other records, to inflate reimbursement. —There are also reports some hospitals may be using electronic health records to facilitate ‘_upcoding’ of the intensity of care or severity of patients’ condition as a means to profit with no commensurate improvement in the quality of care, the letter said. Source: <http://www.nytimes.com/2012/09/25/business/us-warns-hospitals-on-medicare-billing.html>

(Texas) West Nile claims another life in Texas. Texas State health officials reported September 25 one new death from West Nile virus in Midland County, bringing to 63 this year's death toll from the disease. The State health department reported 23 new confirmed cases September 24. Statewide, the number of people contracting the potentially fatal West Nile neuroinvasive disease jumped by 13, up from 664 confirmed cases September 24. Another 10 people were confirmed with the less serious West Nile fever, bringing the total to 752 across the State. The latest data published by the Texas Department of State Health Services stated 1,429 people have contracted the mosquito-borne illness this year. Source: http://www.news-journal.com/news/local/west-nile-claims-another-life-in-texas/article_41ce7ba2-6954-57db-ad8b-161a29af6cc3.html

(District of Columbia) Alexandria woman sentenced for selling patient information. A former medical technician at Howard University Hospital in Washington D.C. was sentenced September 21 to 6 months in a halfway house and ordered to perform 100 hours of community service on a federal charge stemming from the sale of personal data about patients and blank prescription forms, said a U.S. attorney and Assistant Director in Charge of the FBI's Washington Field Office. The former technician pled guilty in June in court to the wrongful disclosure of individually identifiable health information. The judge placed her on 3 years of probation. She also was fined \$2,100. She worked as a medical technician in Howard University Hospital's general

UNCLASSIFIED

UNCLASSIFIED

surgery department. From August 2010 through December 2011, on at least three occasions, she obtained records of multiple hospital patients and then sold the names, addresses, dates of birth, and Medicare numbers to another person, along with blank hospital prescription forms. She received about \$500 to \$800 in cash for each of the transactions. In total, she sold about 40 Howard University Hospital patient names and information to the person, and she received approximately \$2,100 in cash in return. Source: <http://fairfaxnews.com/2012/09/alexandria-woman-sentenced-for-selling-patient-information/>

TRANSPORTATION

Nothing Significant to Report

WATER AND DAMS

(Ohio) **Bronze from flood gate discovered stolen.** Crews discovered September 24 that control systems on a flood gate in Dayton, Ohio, were stolen. Bronze parts on the storm system, measuring about 15 to 20 feet long, were removed from the gates recently. Police have notified scrap yards to be looking for the parts. The City of Dayton Water Department said the bronze probably weighed about 3 pounds and may be worth about \$1,800. Source: <http://www.whiotv.com/news/news/bronze-from-flood-gate-discovered-stolen/nSKnG/>

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