

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

Army Corps, Valley City begin flood risk management study. The U.S. Army Corps of Engineers in both Valley City, North Dakota, and Saint Paul District, Minnesota, entered into a formal agreement to partner in a flood risk management study, Dredging Today reported April 3. The Valley City, Sheyenne River Flood Risk Management Feasibility Study will identify measures to reduce average annual flood damages and to reduce flood-related risks to public safety in Valley City. The study partners will evaluate alternatives for flood damage reduction and flood risk management. The study plans to identify an implementable project that will reduce the overall risk of flooding. The study will be developed in coordination with the public and a number of local, state, and federal agencies. The complete study is estimated to cost \$1.5 million and take 2 and a half years to complete. Source:

<http://www.dredgingtoday.com/2012/04/03/army-corps-valley-city-begin-flood-risk-management-study-usa/>

REGIONAL

(Montana) Corps plans Fort Peck spillway test. The U.S. Army Corps of Engineers plans to release 3,000 to 30,000 cubic feet per second (cfs) of water through the Fort Peck Dam spillway in Montana during the summer of 2012 to ensure it is performing properly after 2011's year of high water. The test will help engineers determine whether a subdrain system that relieves pressure beneath the spillway is functioning. "We have concerns about those drains working properly," said the Corps' project manager. The test will take place over 4 days and would raise the water level directly downstream of the dam up to 4.7 feet with the highest test releases of 30,000 cfs. That rise would quickly dissipate the farther downstream the water travels, with the river near Wolf Point rising 1.7 feet. Near Culbertson, the river would rise 1.1 feet. Officials said the drop in the lake level would be insignificant. The public would be given a minimum of 30 days advance notice of the test dates. Source: http://billingsgazette.com/news/state-and-regional/montana/corps-plans-fort-peck-spillway-test/article_83fac5c8-af16-53df-a6d2-c6f4c0a0ddb2.html

(Montana) Oil, gas board to begin 'risk-based' well inspections. The Montana Board of Oil and Gas Conservation — told in a September 2011 legislative audit to improve its inspections and enforcement of oil and gas well operations — asked the petroleum department at Montana Tech to assist in making improvements, the Great Falls Tribune reported April 3. One recommendation in the audit was that the division develop a formal risk-based inspection approach that establishes inspection priorities. Source:

<http://www.greatfallstribune.com/article/20120403/NEWS01/120403007/Oil-gas-board-begin-risk-based-well-inspections?odyssey=nav|head>

(South Dakota) SD forest fire contained. Officials said the Black Hills National Forest fire in southwest South Dakota has been contained. The Forest Service said the fire was contained March 31, after scorching 546 acres. The agency said no structures were threatened and no injuries were reported in the Apple Fire, which was started by lightning March 28. Source:

UNCLASSIFIED

[http://hosted2.ap.org/ALDEC/TDNational/Article 2012-04-01-SD%20Forest%20Fire/id-9f5b1e286e3b4871b9f6862f518cd4cc](http://hosted2.ap.org/ALDEC/TDNational/Article%202012-04-01-SD%20Forest%20Fire/id-9f5b1e286e3b4871b9f6862f518cd4cc)

NATIONAL

DHS: America's water and power utilities under daily cyber-attack. America's water and energy utilities face constant cyber-espionage and denial-of-service attacks against industrial-control systems, according to the team of specialists from the U.S. Department of Homeland Security (DHS) who are called to investigate the worst cyber-related incidents at these utilities, Network World reported April 4. Out of the 17 fly-away trips taken in 2011 by DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to assist utilities in network and forensics analysis, 7 of the security incidents originated as spear-phishing attacks via e-mail against utility personnel. An ICS-CERT leader said 11 of the 17 incidents were very "sophisticated," signaling a well-organized "threat actor." She said DHS believes that in 12 of the 17 cases, if only the compromised utility had been able to practice the most basic type of network security for corporate and industrial control systems, they would likely have detected or fended off the attack. One of the basic problems observed at utilities is that "a lot of folks are using older systems previously not connected to the Internet," she said. Another ICS-CERT leader said the count of "incident tickets" related to reported incidents at water and power-generating utilities is going up. While only 9 incidents were reported in 2009, in 2011 this grew to 198 incident tickets. Just over 40 percent came from water-sector utilities, with the rest from various energy, nuclear energy, and chemical providers. He said in many cases the attacks do not seem to be coming directly through the Internet via Internet Service Providers, for example, but are often traced to outside companies that provide services to the attacked utilities, raising the question of compromises there. Source:

<http://www.networkworld.com/news/2012/040412-dhs-cyberattack-257946.html?page=1>

Internet voting not ready for elections, says DHS official. Unresolved technological problems means Internet voting should not yet be deployed to U.S. elections, a Homeland Security Department cybersecurity official told a conference of election officials and watchdogs. "It's definitely premature to deploy Internet voting in real elections," said the official, speaking before the Election Verification Network conference in Santa Fe, New Mexico, March 29. "The security infrastructure around Internet voting is both immature and under-resourced," he told the audience, citing National Institute of Standards and Technology (NIST) internal reports that summarize technical research on particular subjects. When it comes to end-to-end cryptographic voting techniques, the NIST report states that they "are largely still an academic effort." Source: <http://www.fiercegovernmentit.com/story/internet-voting-not-ready-elections-says-dhs-official/2012-04-02>

INTERNATIONAL

Cracks detected again in Swedish reactor control rods. Small cracks were again detected in control rods used to control the fission process at two nuclear reactors at the Forsmark nuclear power plant in Sweden, media reports said March 28. Cracks were detected in 2011 at one

UNCLASSIFIED

UNCLASSIFIED

reactor at Forsmark and one reactor at the Oskarshamn plant, in south- eastern Sweden. Several control rods were replaced at the end of 2011, but some of the new rods appeared to have faults. Oskarshamn plant's chief executive told Swedish radio news that the new rods may have been damaged at production, but a probe was underway. Source:

<http://www.nucpros.com/content/cracks-detected-again-swedish-reactor-control-rods>

North Sea gas rig blast averted. A flare that threatened to cause an explosion at a North Sea platform has gone out, its operator said March 31, but a plume of highly flammable gas was still leaking from the stricken rig. There had been fears that the cloud of gas, which continues to leak from the platform at a rate of an estimated 200,000 cubic meters per day, could come into contact with the flame and ignite, causing a massive explosion. "There is still a gas escape, and clearly escaping gas is always at risk of ignition and explosion," Total's U.K. communications manager said. A spokesman at the firm's Paris headquarters stated Total was losing revenues of \$1.5 million every day as a result of the shutdown of production at Elgin. The company is preparing to sink two relief wells to stop the gas leak. Source:

<http://www.calgaryherald.com/North+blast+averted/6393190/story.html>

BANKING AND FINANCE INDUSTRY

Phishers use web analytics to gauge success. In yet another indication of cybercriminals operating more like a business, researchers have discovered a major phishing campaign that relied on Web analytics to hone its attack against a bank, Dark Reading reported April 5. Researchers at security firm RSA say a phisher targeting a specific bank in South America used a free Web analytics tool to gather statistics on how his attacks performed and details about his victims' systems. He configured it like any other Web analytics service, using embedded JavaScript code on his Web page visited by victims who fell for the phishing attack. The code records data such as the number of "hits" on the page, as well as specifics like the user's operating system and browser type. A communications specialist for RSA's FraudAction Knowledge Delivery said the attacker can glean plenty of valuable information from Web analytics: traffic trends and intelligence on the best time to send out its spam phishing run. "Using Web analytics stats, they can - 8 - get quite a bit of information: number of hits — how credible was the spam e-mail?; best time for blasting out their campaigns — night/weekends?; pages viewed per visitor — did the consumer go through the whole phishing kit?; success of a particular spam e-mailing list they've purchased; or the success of an underground spamming service they've paid for," she said. Source: <http://www.darkreading.com/insider-threat/167801100/security/client-security/232800400/phishers-use-web-analytics-to-gauge-success.html>

IRS security dissing party continues. The U.S. Internal Revenue Service's (IRS) Computer Security Incident Response Center (CSIRC), set up to monitor IRS networks, is failing to monitor 34 percent of the agency's servers, according to a Treasury audit, Infosecurity reported April 4. In the audit released March 2012, the Treasury Inspector General for Tax Administration (TIGTA) found that, in addition to not monitoring all of the IRS servers, the CSIRC was not reporting all computer security incidents to the Treasury as required. Also, IRS computer

UNCLASSIFIED

UNCLASSIFIED

incident response policies, plans, and procedures —are either nonexistent or are inaccurate and incomplete. To remedy the center’s shortcomings, the TIGTA recommended the IRS’ assistant chief information officer for cybersecurity direct the CSIRC to develop its cybersecurity data warehouse capabilities to correlate and reconcile active servers connected to the IRS network with servers monitored by the host-based intrusion detection system; revise and expand the agreement with the TIGTA to ensure all reportable and relevant security incidents are shared with the CSIRC; collaborate with the TIGTA to create common identifiers to help the CSIRC reconcile its incident tracking system with TIGTA; develop a stand-alone incident response policy or update the policy in the IRS’s manual with current and complete information; develop an incident response plan; and develop, update, and formalize all critical standard operating procedures. Source: <http://www.infosecurity-magazine.com/view/24979/irs-security-dissing-party-continues/>

RBC sued by U.S. regulators over wash trades. Royal Bank of Canada (RBC) was sued April 2 by U.S. regulators over claims that the Toronto, Canada-based lender engaged in illegal futures trades worth hundreds of millions of dollars to garner tax benefits tied to equities. Canada’s biggest bank made false and misleading statements about “wash trades” from 2007 to 2010 in which affiliates traded among themselves in a way that undermined competition and price discovery on the OneChicago LLC exchange, the Commodity Futures Trading Commission (CFTC) said in a complaint filed in a New York federal court. Royal Bank enlisted affiliates to help carry out hundreds of futures transactions that were done off-exchange and then reported to OneChicago as block trades between independent affiliates, according to the CFTC. The trades, which resulted in Royal Bank not having a financial position in a market, were conducted for Canadian tax benefits tied to holding certain stocks, the CFTC said. The transactions, involving single-stock futures and narrow-based indexes, were used to hedge the risk of holding the equities, according to the statement. Between 2006 and 2010, the narrow-based index - 6 - trades between a Toronto-based bank account and RBC Europe Ltd., a London-based bank subsidiary, represented all of the narrow-based index volume on OneChicago, the CFTC said in the complaint. Senior members of the bank’s central funding group determined the prices and contracts traded. From 2005 to 2010, RBC concealed material information and made false statements about the trades to CME Group Inc., which had regulatory oversight of the exchange, according to the CFTC. RBC’s responses to CME questions about the trades “concealed information concerning the central role” of the central funding group and the bank’s single-stock futures trades, CFTC said. The CFTC is seeking monetary penalties and an injunction against further violations, the agency said. Source: <http://www.businessweek.com/news/2012-04-02/rbc-sued-by-u-dot-s-dot-regulators-over-wash-trades-seeking-tax-benefit>

1.5 million card numbers at risk from hack. A data breach at a payments processing firm potentially compromised up to 1.5 million credit and debit card numbers from all of major card brands. Global Payments, a company that processes card transactions, confirmed March 30 that “card data may have been accessed.” It said it discovered the intrusion in early March and “promptly” notified others in the industry. Global Payments released a statement April 1 with more details. The company said that while more than 1 million card numbers were potentially

UNCLASSIFIED

UNCLASSIFIED

compromised, cardholder names, addresses, and Social Security numbers were not affected. Global Payments did not say which card companies were affected, but Visa released a statement March 30 saying it was all of the major companies. MasterCard said it alerted payment card issuers “regarding certain MasterCard accounts that are potentially at risk.” Discover and American Express said they are monitoring the situation. Global Payments held a conference call April 2 to provide more details on the debacle. Executives stressed that an investigation is ongoing. Until the investigation is complete, they are waiting to release specifics on how the hack occurred. A U.S. Secret Service spokesman said March 31 the agency also is investigating the incident. Global Payments said the breach was limited to only “a handful of servers,” and appears to be confined to accounts in North America. Global Payments processed \$167 billion worth of transactions in its last fiscal year. Source:

<http://money.cnn.com/2012/04/02/technology/global-payments-breach/>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

EPA holds off on oil, gas proposals. The U.S. Environmental Protection Agency (EPA) said it was delaying air pollution standards for hydraulic fracturing while it weighed thousands of public comments. The EPA had until April 3 to finalize air pollution standards for oil storage tanks, compressors, and natural gas wells developed by hydraulic fracturing, also known as fracking. It opted to delay the rules for 2 weeks. “EPA and parties have agreed to a two-week extension on a consent decree to issue final air emission rules for the oil and natural gas industry,” the agency said in a statement. “The agency requested the additional time to fully address the issues raised in the more than 156,000 public comments we received on the proposed rules.” The EPA said the new rules would decrease by more than 90 percent the emissions of volatile organic compounds from hydraulically fractured natural gas wells. Volatile organic compounds are tied to cancer and smog formation. Source: http://www.upi.com/Business_News/Energy-Resources/2012/04/03/EPA-holds-of-on-oil-gas-proposals/UPI-63471333454233/

COMMERCIAL FACILITIES

(Texas) ‘Robotic device’ triggers evacuation at Dallas Love Field. Dallas Love Field in Texas was shut down April 1 after a Southwest Airlines jet bound for Amarillo was found with a suspicious device on board. The Transportation Security Administration said passengers were evacuated from Gates 3 to 15 “out of an abundance of caution.” A City of Dallas spokesman said a “robotic device” was found near the cockpit of Southwest Airlines Flight 157 after it arrived from Kansas City. Air marshals and Love Field security officers detained 11 passengers — including students and their professor — who were linked to the gizmo. “It was determined that the device was not dangerous and was a student’s science project,” the spokesman said in a written statement. “The student told authorities the robot was accidentally left on the plane.” Source: <http://www.wfaa.com/news/local/Love-Field-evacuation-was-false-alarm-145697115.html>

UNCLASSIFIED

COMMUNICATIONS SECTOR

Fake AT&T wireless bill links to malware. Large outbreaks of phony AT&T wireless e-mails were distributed in the last 2 days, Commtouch said April 5. The e-mails describe very large balances (\$943), that are sure to get aggravated customers clicking on the included links. Every link in the e-mail leads to a different compromised site with malware hidden inside. The pattern is: legitimate domain / recurring set of random letters / index.html. The index.html file tries to exploit at least the following known vulnerabilities: Libtiff integer overflow in Adobe Reader and Acrobat — CVE-2010-0188; and Help Center URL Validation Vulnerability — CVE-2010-1885. Source: http://www.net-security.org/malware_news.php?id=2057

PBS website hacked by Anonymous, passwords dumped. Anonymous hackers claimed to have breached the Web site of the Public Broadcasting Service (pbs.org), leaking large amounts of sensitive information from its databases, Softpedia reported April 2. One of the dump files, published on Pastebin, contained around 300 usernames and password hashes that can allegedly be used to access the site's database. Another post held close to 200 record sets that represent "stations and password." It was uncertain as of April 2 what the passwords access, but the file also contained TV station names, Web site URLs, e-mail addresses, physical addresses, and contact details. A number of 1,600 usernames, clear-text passwords, and e-mail addresses that belong to the members of the press were also leaked. A separate file showed the usernames, names, e-mail addresses, and password hashes of Web site administrators, totaling a number of 38 records, and another one, entitled "logins" held 250 names, usernames, e-mail addresses, and passwords. The site was previously hacked two times in 2011. Source: <http://news.softpedia.com/news/PBS-Website-Hacked-by-Anonymous-Passwords-Dumped-262195.shtml>

CRITICAL MANUFACTURING

Chinese hedge and grass trimmers recalled following reports of fuel leaks. Thousands of Chinese-made grass and hedge trimmers were recalled due to fuel tank leaks, according to a Consumer Product Safety Commission announcement April 4. Trimmers made by Husqvarna Machinery Manufacturing Co. Ltd. were found to leak between the fuel line and the tank. No injuries were reported. The commission said the trimmers should be returned to the place of purchase for a free repair. The recall included about 19,500 grass trimmers and 6,500 hedge trimmers that were sold from May 2011 to January 2012. Source: http://www.washingtonpost.com/business/chinese-hedge-and-grass-trimmers-recalled-following-reports-of-fuel-leaks/2012/04/04/gIQALTtHvS_story.html

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

(California) LAPD radio system fails for 12 hours. The Los Angeles Police Department (LAPD) radio communications was down for half the day April 3. A city councilman said he will call for the dismissal of the General Services Department general manager for the power outage at Mount Lee, where all LAPD radio communications equipment is housed. The city councilman said General Services crews were sent to the Mount Lee facility to test a backup generator. He said the test failed and knocked out all power at Mount Lee, shutting down radio communications, placing —the public and officers at extreme risk. LAPD officials and the Mayor’s Office said backup systems were used that ultimately prevented any serious breakdowns in communication. According to the councilman, the communications breakdown meant a delayed response to emergencies, as 9-1-1 calls had to be answered manually with operators then calling stations to dispatch an officer. For officers, he said, the danger came in the form of an inability to get immediate access to information, such as a driver history based on license plates. Source: http://www.dailynews.com/politics/ci_20329374/lapd-radio-system-fails-12-hours

(Alabama; Texas) Feds charge confessed Anon member after tracking his digital footprints. April 4, Ars Technica reported that a Texas man was criminally charged with taking part in a string of hacks that targeted government and law-enforcement Web sites under the banner of —CabinCr3w, an offshoot to the Anonymous hacking collective. The Linux administrator from Galveston, Texas, was charged with unauthorized access to a protected computer, according to documents filed in U.S. District Court in Austin. His hacks, under a campaign his group took to calling —Operation Pig Roast, allegedly penetrated sites operated by at least four law-enforcement groups and in some cases dumped phone numbers, addresses, and other personal information belonging to police officers. He was also accused of hacking into the County of Houston’s Web site in Alabama. Source: <http://arstechnica.com/business/news/2012/04/feds-charge-self-confessed-anonymous-member-after-tracking-his-digital-footprints.ars>

(Indiana) Bloomington man called hero in deputy struggle. The Monroe County Sheriff’s Department is crediting a Bloomington, Indiana man for saving a deputy’s life, WRTV 6 Indianapolis reported March 30. A sheriff’s deputy was with a suspect en route to the Monroe County Jail when detectives said the suspect somehow got his handcuffs in front of his body while in a seat belt in the back of the deputy’s SUV and brought his arms around the deputy’s neck, and then reached for her gun. The gun went off, narrowly missing the deputy’s leg. A man nearby said he heard the deputy scream and rushed to help. “I opened the door and jumped on (the suspect’s) back. I put him in a headlock and pried him off (the deputy),” he said. The man tore a ligament in his hand during the violent struggle and said he heard the suspect tell the deputy she “Wouldn’t get out of the car alive.” Monroe County Sheriff’s Department officials also commended the man and said they expect he will be formally recognized by the sheriff. Source: <http://www.theindychannel.com/news/30805597/detail.html>

ENERGY

Serious cybersecurity lapses found at Pacific Northwest electricity supplier. The Department of Energy (DOE) identified serious cybersecurity gaps at the Bonneville Power Administration, which supplies wholesale electric power to regional utilities in the Pacific Northwest, Infosecurity reported March 30. An audit by DOE's Office of the Inspector General (OIG) found Bonneville did not implemented controls designed to address known IT system vulnerabilities. "Specifically, technical vulnerability scanning conducted on nine applications used to support business functions such as financial management, human resources, and security management identified a significant number of high-risk weaknesses in the areas of access controls, patch management, and validation of user input," according to the audit. In addition, OIG's testing of five operational security control systems identified issues with configuration management, access controls, and contingency and security planning. A number of IT system development efforts suffered from cost, scope, and schedule overruns due to weaknesses in project planning and management. Source: <http://www.infosecurity-magazine.com/view/24869/serious-cybersecurity-lapses-found-at-pacific-northwest-electricity-supplier/>

FOOD AND AGRICULTURE

BC issues warning about pomeberry frozen berries. Eight cases of hepatitis A over the past 2 months in British Columbia may be linked to frozen berries, the British Columbia Center for Disease Control (BCCDC) said April 5. It warned consumers not to eat Pomeberry Blend frozen berries manufactured by Western Family. The blend, which was distributed through Save-On-Foods and Overwaitea, contains frozen pomegranate seeds, blueberries, strawberries, - 10 - and cherries. According to the news release, five of the eight people ill with the virus are known to have consumed the Pomeberry product. Although there is no direct link yet, the BC health authorities suggest as a precaution, individuals who have the Pomeberry Blend product in their refrigerator or freezer should not to consume it and should discard it. At this time, the BCCDC thinks the overall risk to the public is very low, and it is not recommending that people who have consumed the product should receive vaccine. Source: <http://www.foodsafetynews.com/2012/04/bc-issues-warning-about-pomeberry-frozen-berries/>

Final report on Jimmy John's E. coli outbreak: 29 ill in 11 states. The Centers for Disease Control and Prevention (CDC) issued a final report on the multistate outbreak of E. coli infection linked to sprouts in Jimmy John's sandwiches, Food Safety News reported April 3. Between late December 2011 and early March, 29 individuals were infected with E. coli O26 traced to raw clover sprouts from Jimmy John's Gourmet Sandwich restaurants. The case count in the Final Case Update is up 4 from the last update March 8, which identified 25 victims. Three of the new cases were from states that had not reported any outbreak-related illnesses as of March. Those states — Pennsylvania, Washington, and West Virginia — each reported one case. Michigan's victim count rose from 2 to 3. The final breakdown of cases by state is as follows: Alabama (1), Arkansas (1), Iowa (5), Kansas (2), Michigan (10), Missouri (3), Ohio (3), Pennsylvania (1), Washington (1), Wisconsin (1), and West Virginia (1). Of the 27 victims interviewed, 85 percent

UNCLASSIFIED

reported eating sprouts at Jimmy John's in the 7 days before their symptoms began. Source: <http://www.foodsafetynews.com/2012/04/final-report-on-jimmy-johns-e-coli-outbreak-released/>

Deadly citrus disease turns up in California. A citrus disease that has killed millions of citrus trees and cost growers billions of dollars across Florida and Brazil has been detected in California, despite the industry's best efforts to keep it at bay, the Associated Press reported April 1. After a week of testing the U.S. Department of Agriculture confirmed citrus greening was detected in a lemon-grapefruit hybrid tree in a residential neighborhood of Los Angeles County. The disease stands to threaten not only California's nearly \$2 billion citrus industry but backyard trees scattered throughout the state. "Huanlongbing is called the world's worst disease of citrus," said an official with the California Department of Food and Agriculture. The bacterial disease is carried by the Asian citrus psyllid and attacks a tree's vascular system, producing bitter fruit and eventually killing the tree. Sap-sucking psyllids that feed on an infected tree become carriers of the disease. The disease is present in Mexico and across the southern U.S., but nowhere is the problem more severe than in Florida, where the disease first appeared in 2005. The University of Florida estimates it has cost 6,600 jobs, \$1.3 billion in lost revenue to growers, and \$3.6 billion in lost economic activity. The pest and the disease also are present in Texas, Louisiana, Georgia, and South Carolina. The states of Arizona, Mississippi, and Alabama have detected the pest but not the disease. Source: <http://nhregister.com/articles/2012/04/01/news/doc4f7908eb4ddbc220182535.txt>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Iowa) Iowa Capitol opened after powder prompts lock down. Authorities locked down the Iowa Statehouse in Des Moines for several hours April 3 after a legislator opened an envelope containing a suspicious white powder and a threatening letter. The representative opened the envelope on the House floor, and lawmakers quickly sought the advice of the Iowa State Patrol. Officers ordered that the Statehouse be closed while postal inspectors, and a Des Moines hazardous materials crew rushed to the building. About 4 hours later, officers announced the powder was deemed harmless and people could leave the building. Source: <http://www.wtop.com/?nid=209&sid=2813766>

(California) Oakland university shooter was hunting staff member refused to refund his tuition, police say. The man accused of slaughtering seven people at Oikos University in Oakland, California, was hoping to find and kill an administrator who no longer works at the school, police said April 5. The suspect — who is reported to have confessed to the April 2 killing spree — was angry that the woman who refused him a full refund of his \$6,000 tuition fees when he dropped out of his nursing classes late in 2011, the Oakland Tribune reported. Police said the woman left the school soon after the suspect. When he failed to find the woman, the suspect instead killed six students and a receptionist with a semiautomatic handgun. He reportedly also wounded three other people, before stealing a victim's car and

UNCLASSIFIED

UNCLASSIFIED

driving to nearby supermarket where he admitted his crimes to staff and was arrested, officials said. He is charged with seven counts of murder and related offenses. Source:

<http://www.foxnews.com/us/2012/04/06/oakland-university-shooter-was-hunting-staff-member-refused-to-refund-his/>

(California) Police: California shooting suspect shows no remorse. The man accused of killing seven people execution-style at a small religious college in Oakland, California, “does not appear to be remorseful at all,” the city’s police chief said April 3. The former student, told authorities he was upset at being expelled from Oikos University, the police chief said. He was upset - 13 - with some administrators and students and said he had been “picked on” and “wasn’t treated fairly,” he said. Investigators believe the suspect walked into the single-story building housing the university April 2, took a receptionist hostage, and went looking for a particular female administrator, who was not there. After the shooting, the man left the classroom, reloaded his semi-automatic weapon, and returned, firing into several classrooms, the police chief said. He ended his rampage by driving off in a victim’s car. In all, seven people were killed and three were wounded. “This happened within minutes,” the police chief said. “We don’t think the victims had any opportunity to resist, any opportunity to surrender.” The suspect was arrested a short time after the shooting, when he surrendered to police at a grocery store in the Oakland suburb of Alameda, police said. Police expect to present the case to the district attorney for possible charges later in the week of April 2.

Source: <http://www.cnn.com/2012/04/03/us/california-shooting/>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Fast-growing Flashback botnet includes over 600,000 Macs, experts say. More than 600,000 Macs have been infected with a new version of the Flashback trojan being installed on people’s computers with the help of Java exploits, security researchers from antivirus vendor Doctor Web said April 4. Flashback is a family of Mac OS malware that appeared in September 2011. Older Flashback versions relied on social engineering tricks to infect computers, but the latest variants are distributed via Java exploits that do not require user interaction. April 3, Apple released a Java update in order to address a critical vulnerability being exploited to infect Mac computers with Flashback. However, a large number of users have already been affected by those attacks, Doctor Web said in a report issued April 4. The company’s researchers managed to hijack a part of the Flashback botnet through a method known as sinkholing, and counted unique identifiers belonging to more than 550,000 Mac OS X systems infected with the trojan. Over 300,000 of the Flashback-infected Macs, or 56 percent of the total, are located in United States, while over 100,000 are located in Canada, Doctor Web said. The United Kingdom and Australia are next, with 68,000 and 32,000 infected Macs, respectively. The botnet is growing at a rapid rate. Hours after Doctor Web issued its report, one of the company’s malware analysts announced the botnet had grown to over 600,000 infected computers. He also said 274 Macs infected with the new Flashback variant were located in Cupertino, the U.S. city where Apple has its headquarters. Source:

http://www.computerworld.com/s/article/9225862/Fast_growing_Flashback_botnet_includes_over_600_000_Macs_experts_say?source=rss_security&utm_source=feedburner&utm_medium=

UNCLASSIFIED

UNCLASSIFIED

[m=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+\(Computerworld+Security+News\)&utm](http://www.computerworld.com/s/feed/topic/17+(Computerworld+Security+News)&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm)

Path tightens mobile app security. Social networking service Path upgraded the security of its mobile application in apparent response to a recent outcry over its data gathering practices. In a statement, Path said a newly released 2.1.1 version of its software automatically hashes all user contact information in order to protect the privacy of the data. All phone numbers, e-mail addresses, Twitter handles, and Facebook IDs Path collects in order to connect users with their contacts will be hashed in future, according to the statement. Path's move comes several weeks after the company found itself in the middle of a major privacy row after a programmer described how Path's journaling application for iOS and Android-powered phones, used by over 2 million users, was secretly collecting user address book data. The disclosure drew widespread attention to the data collection practices of mobile application vendors in general, and the processes platform vendors such as Apple and Google use for vetting those vendors. Source: http://www.computerworld.com/s/article/9225819/Path_tightens_mobile_app_security

Cybercriminals target Google, LinkedIn and Mass Effect 3 users. During March, GFI Labs documented several spam attacks and malware-laden e-mail campaigns infiltrating users' systems under the guise of communications purporting to be from well-known companies and promotions for popular products and services. Google, LinkedIn, Skype, and the video game Mass Effect 3 were among the brands exploited by cybercriminals in order to attract more victims. "Taking advantage of the notoriety of companies, celebrities and major events is a tactic cybercriminals continue to use because it works," said a senior threat researcher at GFI Software. "They know that Internet users are bombarded with countless emails every day, and these scammers prey on our curiosity and our reflex-like tendency to click on links and open emails that look like they're coming from a company we know and trust," he added. Source: [http://www.net-security.org/malware_news.php?id=2055&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+\(Help+Net+Security\)&utm_content=Google+Reader](http://www.net-security.org/malware_news.php?id=2055&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader)

Anonymous and Lulzsec hackers evolving to target corporate data to cause financial pain. Hacker groups Anonymous and LulzSec are changing tactics to target firms' corporate data in order to hurt them financially, rather than cause embarrassment by affecting Web sites, according to new research from security firm Imperva. In its latest Hacker Intelligence Initiative report, Imperva researchers said they saw a marked change in hacktivists' behavior, with groups moving away from defacing Web sites or knocking them offline to stealing data. Specifically, Imperva researchers reported discovering that 21 percent of all recorded incidents from June to November 2011 saw hackers mounting local and remote file inclusion (RFI/LFI) attacks. The statistic was widely attributed to hacktivists, such as the Anonymous collective and LulzSec group. A form of attack that targets PHP coding, the use of RFI/LFI techniques allows hackers to steal data by manipulating the company's Web server, and indicates a step away from their usual tendency to target companies' Web sites with distributed denial-of-service assaults. Source: <http://www.v3.co.uk/v3-uk/news/2165469/anonymous-lulzsec-hackers-evolving-target-corporate-cause-financial-pain>

UNCLASSIFIED

UNCLASSIFIED

Facebook logins easily slurped from iOS, Android kit. Facebook's iOS and Android clients do not encrypt users' logon credentials, leaving them in a folder accessible to other apps or USB connections. A rogue application, or 2 minutes with a USB connection, is all that is needed to steal the temporary credentials from either device. In the case of iOS, someone can even take the data from a backup, enabling the hacker to attach to a Facebook account and access applications. This exploit comes from a reader of The Register, who came across the file and tested it to see if it was easy enough to pretend to be someone else. After developing a proof-of-concept, which lifted "several thousand" IDs, the reader deleted the collected data and reported the matter to Facebook. It appears Facebook is already aware of the problem and working on a fix — though it will not say how long it is going to take or what users should do in the meantime. Source:

http://www.theregister.co.uk/2012/04/03/facebook_security_weak_logon/

Adobe releases open source malware classification tool. Adobe Systems released a malware classification tool in order to help security incident first responders, malware analysts, and security researchers more easily identify malicious binary files. The Adobe Malware Classifier tool uses machine learning algorithms to classify Windows executable and dynamic link library files as clean, malicious, or unknown, a Adobe security engineer said. When run, the tool extracts seven key attributes from every analyzed binary file and compares them to data obtained by running the J48, J48 Graft, PART, and Ridor machine-learning algorithms on a set of 100,000 malicious programs and 16,000 clean ones, he said. Source:

http://www.computerworld.com/s/article/9225778/Adobe_releases_open_source_malware_classification_tool

Fake US Airways emails lead to Zeus variant. A US Airways-themed spam campaign aiming at infecting users with a variant of the Zeus banking trojan has been hitting inboxes for the last 2 weeks, according to a Kaspersky Lab researcher. This particular spam e-mail purportedly contains the confirmation code and the online reservation details needed for the users to confirm their flight reservation. However, the offered links take users to one of a number of compromised domains containing malicious javascripts that perform a number of redirections and finally land the victims on a domain hosting the BlackHole exploit kit. Once the kit exploits a vulnerability in Java, Flash Player, or Adobe Reader, a downloader that ultimately connects to a command and control server and downloads and runs the GameOver Zeus variant is installed on the machine. "At all the stages of this attack, every object — domains, links to javascripts, files with exploits, the downloader and Zeus — was frequently replaced with a new one," the researcher said. "The domains remained 'alive' for nearly 12 hours, while the Zeus samples were replaced more often." Given that the exploits, downloaders, and Zeus modifications used by the cybercriminals in this attack were detected mostly by Russian, U.S., Italian, German, and Indian Kaspersky users, the researcher speculates the spam campaign is not the only method used by these cyber crooks to spread Zeus. Source: http://www.net-security.org/malware_news.php?id=2054&utm

UNCLASSIFIED

UNCLASSIFIED

Expert shows how hackers can use CSRF browser vulnerability. The hacker who broke into GitHub to demonstrate a vulnerability warns that cross-site request forgery (CSRF), a security hole that affects all browsers, must be addressed immediately because it poses a great risk for unsuspecting users. He claims CSRF security holes have been present for a long time, but many underestimated the dangers hiding behind them. Unlike cross-site scripting attacks which exploit the trust of a user towards a particular site, CSRF attacks rely on the trust that a site has in a browser. The expert explains that when users sign in to any site, dubbed by the researcher as site1.com, they are remembered by the cookie mechanism. By leveraging the vulnerability, the hacker can shorten the Web site's session and social engineer the victim into signing in again. The user signs in the second time and a malicious script is triggered. Then, when the user visits a second site, named site2.com, the exploit begins. Source:

<http://news.softpedia.com/news/Expert-Shows-How-Hackers-Can-Use-CSRF-Browser-Vulnerability-262109.shtml>

Potential first Android bootkit spotted. Security researchers of NQ Mobile recently discovered what might be the first Android bootkit. Dubbed DKFBootKit, the malware piggybacks malicious payloads into legitimate apps that require root privilege. "Specifically, by taking advantage of the root privilege, DKFBootKit adds itself as a part of the boot sequence of the original Android system and replaces a number of utility programs (e.g., ifconfig and mount)," claim the researchers. "By doing so, the malware can get started even before the entire Android framework is bootstrapped." The apps targeted for repackaging with the malicious payload are mostly utility apps, but a few are also apps that provide license keys for some paid apps. The malware's final goal is to make itself run earlier than the Android framework, and to deliver a bot payload that connects the device to several command and control servers and waits to receive additional commands. Source: [http://www.net-security.org/malware_news.php?id=2051&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+\(Help+Net+Security\)&utm_content=Google+Reader](http://www.net-security.org/malware_news.php?id=2051&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader)

Security vulnerability at TweetDeck. The TweetDeck Twitter client apparently suffered from a security breach March 30 that gave some users the ability to take over other people's accounts. Twitter, which owns TweetDeck, reacted quickly and disabled the client's access to the system. TweetDeck's functionality was restored less than a day later, once the bug was fixed. A TweetDeck user discovered the bug which gave him access to the Twitter and Facebook accounts of hundreds of other TweetDeck users. TweetDeck allows its users to pull together both Twitter and Facebook accounts under a TweetDeck account to aggregate updates from both services. The user publicly reported the problem on Twitter, posting a screenshot to document the vulnerability. To back up his claims, he also posted several messages from other people's accounts. In a statement to VentureBeat and other U.S. media, Twitter representatives said no account passwords were compromised and, as far as Twitter is aware, the vulnerability was not exploited maliciously. Facebook told the Wall Street Journal that fewer than 250 of its users were affected, no abuse of those accounts occurred, and it was working with Twitter to "understand the full scope of this issue." Source: <http://www.h-online.com/security/news/item/Security-vulnerability-at-TweetDeck-1498585.html>

UNCLASSIFIED

NATIONAL MONUMENTS AND ICONS

Nothing Significant to Report

POSTAL AND SHIPPING

(California) Postal service offers \$50,000 reward in Planada robbery. The U.S. Postal Service is offering a \$50,000 reward for information leading to the arrest of someone armed with a handgun who robbed one of its drivers March 30 in Planada, California. Federal investigators have not released specific details about the robbery or whether any money or property was taken. The driver, who was contracted through the U.S. Postal Service, was not hurt. Investigators from the Fresno and Stockton offices of the U.S. Postal Inspection Service are working with state and local authorities in the investigation. Source: <http://www.mercedsunstar.com/2012/04/06/2298525/postal-service-offers-50000-reward.html>

(Massachusetts) Suspicious powder found in nearly a dozen mailboxes. A possible April Fool's joke had several state and local authorities responding to nearly a dozen calls of white powder in mailboxes in Hubbardston, Massachusetts, April 1. Police said they received a 9-1-1 call from a resident who claimed to have a bag of white powder in her mailbox. When officers arrived and began to inspect, more than a dozen other mailboxes on the street were discovered with the same contents. The Massachusetts State HAZMAT Team arrived and carefully secured the bags. It was later determined that the substance inside was harmless. Source: <http://www.thebostonchannel.com/r/30812974/detail.html>

PUBLIC HEALTH

ADHD drug shortage to end soon. After months of Americans being unable to fill their drug prescriptions for medications that are commonly used to treat attention deficit hyperactivity disorder (ADHD), the U.S. Food and Drug Administration said April 5 the shortages are expected to end before May. Many ADHD medications, such as Adderall, have been in short supply since 2011. Source: <http://psychcentral.com/news/2012/04/06/adhd-drug-shortage-to-end-soon/37059.html>

(Washington) Whooping cough cases reach epidemic levels in Washington. April 3, the state secretary of health announced whooping cough disease has reached epidemic levels in Washington. So far in 2012, 640 cases have been reported in 23 counties as of March 31. This compares to 94 cases during this same time period in 2011, putting Washington on pace to have the highest number of reported cases in decades. The State Department of Health is introducing a new public service radio announcement reminding people how serious whooping cough can be and to get vaccinated. Source: http://www.doh.wa.gov/Publicat/2012_news/12-038.htm

UNCLASSIFIED

(Wisconsin) Homemade bomb causes fire outside Planned Parenthood clinic. A Planned Parenthood clinic in Wisconsin was closed after a homemade bomb was placed outside the building April 1, the state organization said. The explosive device caused a small fire by the time Grand Chute fire officials arrived, the president and CEO of Planned Parenthood of Wisconsin said in a statement. No patients or staff members were at the health care center at the time. Police in Grand Chute are investigating the incident. Source: <http://edition.cnn.com/2012/04/02/justice/wisconsin-planned-parenthood/index.html>

(Florida) Poison from suicide attempt shuts down Florida emergency room, sickens paramedics. The emergency room at a Margate, Florida hospital was temporarily shut down for roughly 7 hours April 1 after a man who had attempted suicide vomited up poison, sickening three paramedics. The South Florida Sun-Sentinel reported that emergency rescue workers responded to a home of a man who tried to kill himself by drinking pesticide. As the paramedics transported the man to Northwest Medical Center he vomited, causing the rescuers “to become dizzy, nauseous” and suffer headaches. The man was brought into a containment area and the emergency room was closed as a precaution. The vehicle that transported the man to the hospital was put into quarantine. A hazardous materials team from the Broward Sheriff’s Office was called to the scene, and the three paramedics were treated for contamination sickness. Source: <http://www.foxnews.com/us/2012/04/01/poison-from-suicide-attempt-shuts-down-florida-emergency-room-sickens/>

TRANSPORTATION

TSA urged to review plastic airline handcuffs. The chair of the House Homeland Security Committee said March 30 that “use of plastic restraints will be one of the many things that will be fully investigated,” and asked the Transportation Security Administration (TSA) to review security procedures after plastic handcuffs apparently failed to subdue a disturbed pilot on a flight from New York City to Las Vegas March 27, Newsday reported March 31. There is no federal requirement that aircraft have restraints such as plastic handcuffs on board, although airlines and independent aviation security experts said it is industry practice to carry such devices and that flight crews are trained in how to use them. An airline consultant with more than 40 years in the industry, said the failure of the handcuffs on JetBlue Flight 191 appears to be a manufacturing problem. The restraints are routinely used successfully and the government does not need to change its hands-off approach. “The times that I have been involved in their use, they have worked very well,” the airline consultant stated. A JetBlue spokeswoman said crews are trained to use “strengthened plastic flex-cuffs.” The devices, the spokeswoman said, are approved by government regulators. Source: <http://www.heraldnet.com/article/20120331/NEWS02/703319926>

WATER AND DAMS

(Kansas) Drought drying out Kansas aquifers. According to the Kansas Geological Survey (KGS), the lack of rainfall in Kansas in 2011 led to intense declines in ground water levels around the state, the Associated Press reported April 4. KGS said the Ogallala Aquifer in southwest Kansas

UNCLASSIFIED

UNCLASSIFIED

usually sees annual declines, but its average drop of 3.78 feet in 2011 was one of the worst in decades, compared to a drop of about 3 feet in 2010 and 1.39 feet in 2009. Much of Kansas received 25 to 50 percent of normal precipitation in 2011. "The growing season was probably the worst since the 1930s," said a water data manager for the geological survey. In central and south-central Kansas, where ground water levels usually show gains or only modest declines, the water table in the Equus Beds aquifer decreased an average of 3.17 feet. The Big Bend region just west of the Equus Beds had a decline that averaged 3 feet. Farmers in the Big Bend district took out 1,056 emergency permits through the Kansas Department of Agriculture to overpump in 2011, the most out of any district. Source:

<http://www.kansascity.com/2012/04/04/3534830/drought-drying-out-kansas-aquifers.html>

(Georgia) Father of dam explosive suspect arrested. Authorities in Albany, Georgia, arrested the father of a man who was caught with explosives April 2 at the Georgia Power Dam. The father was held on 6 counts of possessing a destructive device April 3. His son was released from jail after making bond April 2. Source: <http://www.walb.com/story/17317128/father-of>

(Georgia) Georgia Dam explosive device suspect released on bond. A man caught with explosives near the Georgia Power Dam in Albany, Georgia, April 1, was released on bond the following day. The man was arrested after police got a tip that someone had explosives near the dam. Dougherty County Police found five explosive devices in the man's car. The Dougherty County police captain said, "Right now we don't have anything to indicate that he is some kind of terrorist, but we really don't know for sure, and that's why we are continuing to look into him and his background." Samples of the explosive device and the chemicals used were sent to the FBI while the rest were destroyed by the Georgia Bureau of Investigation. Source:

<http://www.walb.com/story/17314884/georgia-dam-explosive-device-suspect-released-on-bond>

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center: 866-885-8295 (IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.**

To contribute to this summary or if you have questions or comments, please contact:

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

UNCLASSIFIED