

UNCLASSIFIED



# NORTH DAKOTA HOMELAND SECURITY ANTI-TERRORISM SUMMARY



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

UNCLASSIFIED

## **NDSLIC DISCLAIMER**

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

## **QUICK LINKS**

[North Dakota](#)

[Regional](#)

[National](#)

[International](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials  
Sector](#)

[Commercial Facilities](#)

[Communications Sector](#)

[Critical Manufacturing](#)

[Defense Industrial Base Sector](#)

[Emergency Services](#)

[Energy](#)

[Food and Agriculture](#)

[Government Sector \(including  
Schools and Universities\)](#)

[Information Technology and  
Telecommunications](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Public Health](#)

[Transportation](#)

[Water and Dams](#)

[North Dakota Homeland Security  
Contacts](#)

UNCLASSIFIED

## **NORTH DAKOTA**

Nothing Significant to Report

## **REGIONAL**

**(Minnesota) Minnesota reports 12th fungal meningitis case.** Minnesota reported its 12th confirmed case of fungal meningitis in a national outbreak linked to tainted steroids from a Massachusetts pharmacy, the Associated Press reported November 13. The assistant State epidemiologist said the new case is a Twin Cities area man who received an injection at a metro clinic. He said he had some symptoms earlier but got better. However, in the last few weeks, his symptoms including headaches got worse again. Source:

[http://www.necn.com/11/13/12/Minnesota-reports-12th-fungalmeningitis/landing\\_health.html?&apID=d14e802b73a748b49ff0303dd75d3e7d](http://www.necn.com/11/13/12/Minnesota-reports-12th-fungalmeningitis/landing_health.html?&apID=d14e802b73a748b49ff0303dd75d3e7d)

## **NATIONAL**

**(New York) Man indicted in plot to bomb New York Federal Reserve.** A Bangladeshi man was indicted on charges of attempting to blow up the New York Federal Reserve Bank in October with what he believed was a 1,000- pound bomb, court papers made public November 15 show. The grand jury indictment charges him with one count of attempting to use a weapon of mass destruction and one count of attempting to provide material support to a U.S.-designated foreign terrorist organization, al-Qa'ida. He faces life in prison if convicted. The man was arrested October 17 after pulling up to the Federal Reserve and attempting to detonate what he believed to be a van packed with explosives. The explosives had been provided to him by an undercover agent as part of a sting operation, and were never in working condition, federal authorities said. Source: <http://www.wina.com/Man-indicted-in-plot-to-bomb-New-YorkFederal-Rese/11458736?newsId=177914>

## **INTERNATIONAL**

**Top regulator supports re-evaluating earthquake risks at nuclear plants.** Recent earthquakes demonstrate the need for the country's nuclear industry to re-evaluate the geologic hazards facing power plants, a process that has already started, the new chair of the U.S. Nuclear Regulatory Commission (NRC) said the week of November 5. The NRC Chairwoman said in an interview that a spate of natural events shows the importance of further study. In March, the NRC instructed power companies to re-evaluate the seismic and flooding hazards that their power plants face in the wake of the Fukushima crisis and the East Coast earthquake in 2011. Nuclear plants in the eastern and central United States will have until the end of 2013 to finish the re-evaluation, she said. New evaluations for nuclear plants on the West Coast will take until 2015 to complete since they face more varied geologic conditions. Source:

[http://www.washingtonpost.com/business/top-regulator-supports-re-evaluating-earthquake-risks-at-nuclear-plants/2012/11/08/6ae1a43c-2a01-11e2-aaa5-ac786110c486\\_story.html](http://www.washingtonpost.com/business/top-regulator-supports-re-evaluating-earthquake-risks-at-nuclear-plants/2012/11/08/6ae1a43c-2a01-11e2-aaa5-ac786110c486_story.html)

## UNCLASSIFIED

**Cracks at South Korean nuclear plant raise fresh safety concerns.** Tiny cracks were found in tunnels at a nuclear plant in South Korea, increasing concerns about nuclear safety in the country following a recent scandal involving the use of unverified parts, CNN reported November 9. The reactor where the cracks were found will remain offline for weeks as regulators investigate the problem, putting extra strain on South Korea's already stretched power supply going into the winter months. The utility Korean Hydro & Nuclear Power Co. (KHNP) said it detected microscopic cracks in six control rod tunnels at Unit 3 of its Yonggwang nuclear plant in the southwest of the country. "The cracks are not serious and there is no risk of radiation leakage," said the head of the mechanics department at KHNP. The problem was discovered while the reactor was switched off for a regular 36-day maintenance period. But it will now stay out of service for a further 47 days as inspectors seek to determine the cause of the cracks, the South Korean Nuclear Safety and Security Commission said. Source: <http://www.cnn.com/2012/11/09/world/asia/south-korea-nuclear-reactor/>

## **BANKING AND FINANCE INDUSTRY**

**SEC finds problems in review of credit: raters.** Some credit-rating agencies failed to disclose ratings method changes or were lax in following policies on timely downgrades of securities, according to a report issued by the U.S. Securities and Exchange Commission (SEC) November 15. The SEC summarized the results of its annual examination of raters, a requirement under the 2010 Dodd-Frank Act that called for greater scrutiny of ratings agencies following the 2007-2009 financial crisis. The largest ratings firms, Moody's Corp and Standard & Poor's, were criticized for helping to exacerbate the crisis by giving rosy ratings to subprime mortgage securities that quickly turned toxic. The SEC report did not name which firms had violations, but did distinguish between larger versus smaller creditraters. The SEC's exams were conducted on site at all nine raters registered with the SEC. The SEC found that each of the larger raters and two smaller firms failed to follow their own methodologies and policies for determining ratings. Source: <http://www.reuters.com/article/2012/11/15/us-credit-raters/secidUSBRE8AE19420121115>

**Planned cyberattacks on US banks on hold.** The hacker behind a coordinated attack against major U.S. banks such as Bank of America, Chase, Citibank, PNC, Wells Fargo, and nearly two dozen other banks called off the operation after media reports surfaced a month ago exposing the planned attacks, Threat Post reported November 14. Known as vorVzakone, the Russian has pulled back on his attempt to recruit 100 botmasters for massive man-in-the-middle attacks against American banks. Security blog Krebs on Security named vorVzakone as the mastermind behind the wire-fraud campaign. "Based on a communication posted following the media hype, vorVzakone has since given up on his attack plans for now," said the head of business development for online threats managed services at RSA. "As a result, he has retreated to the deeper Web where we believe he may regroup and plan his attack albeit more secretly." The scheme centered around an obscure piece of crimeware known as Gozi-Prinimalka, an offshoot of the Gozi banking Trojan. VorVzakone was recruiting up to 100 participants for the attack, initially planned for the first week of November. A RSA FraudAction research team member said in October that this was the first time a private cybercrime organization recruited outsiders for

UNCLASSIFIED

## UNCLASSIFIED

such an attack. The attackers were promised a cut for their efforts, and were only to be given executable files by vorVzakone, keeping the recruits dependent on him for updates.

Source: [http://threatpost.com/en\\_us/blogs/planned-cyberattacks-us-banks-hold-111412](http://threatpost.com/en_us/blogs/planned-cyberattacks-us-banks-hold-111412)

**10,000 ID fraud gangs active in US, especially the Southeast, study finds.** There are 10,000 active identity theft crime rings across the U.S., with the greatest concentration in a “ring of fraud” that stretches across the Southeast from Virginia to Mississippi, according to a new report by fraud-fighting firm ID Analytics, NBC News reported November 14. A majority of these rings are what the firm calls “Friends & Family” groups, not professional criminal organizations, the report concludes. The rings are most highly concentrated in Washington D.C.; Detroit; Tampa, Florida; Greenville, Mississippi; Macon, Georgia; and Montgomery, Alabama. ID Analytics compiled the results by examining its massive database of credit applications and other identity “risk events,” which includes 1.7 billion entries. The firm cross references credit applications from major banks, auto dealers, wireless firms, and other credit grantors looking for evidence of systematic identity fraud. A “crime ring” was defined by ID Analytics as two or more individuals working in concert, repeatedly submitting fraudulent applications in an attempt to commit fraud. Collusion was determined by noting when multiple members of the rings used similar personal identifying information, such as Social Security numbers, in fraud attempts. Source: <http://redtape.nbcnews.com/news/2012/11/14/15144350-10000-id-fraud-gangs-active-in-us-especially-the-southeast-study-finds?lite>

**Experts investigate malware used in Gozi- Prnimalka campaign against US banks.** In October, RSA revealed that cybercriminals were planning to launch massive trojan attacks against several U.K. banks. Now, Trend Micro researchers analyzed a few samples of the malware that will likely be utilized in the Gozi-Prnimalka campaign, Softpedia reported November 13. One of the samples, BKDR\_URSNIF.B, is designed to monitor its victims’ browsing activities and collect any information related to financial institutions such as Wells Fargo, PayPal, and Wachovia. Another sample, BKDR\_URSNIF.DN, starts by searching for a specific Firefox registry entry. If this entry is found, a file that drops JS\_URSNIF.DJ is created. If the registry is not located, the malware does not steal any information, but it still performs other malicious tasks. JS\_URSNIF.DJ is the JavaScript that is actually responsible for stealing information. It injects itself into specific Web sites and waits for the victims to enter their credentials. Once the information is harvested, it sends it back to its master via HTTP POST requests. According to the researchers, several command and control servers are utilized by these pieces of malware. Experts also managed to retrieve the names of three additional targets by analyzing the malware’s configurations files. TDBank, Firstrade Securities, and optionsXpress are on the list of targets. All of the institutions have been notified. Source: <http://news.softpedia.com/news/Experts-Investigate-Malware-Used-in-Gozi-Prnimalka-Campaign-Against-US-Banks-306535.shtml>

## **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

Nothing Significant to Report

UNCLASSIFIED

## **COMMERCIAL FACILITIES**

**(New York) Feds: NY man planted Home Depot bomb to extort \$2M.** An employee planted a working pipe bomb in the lighting department of a Huntington, New York Home Depot as part of a plot to extort \$2 million from the company, a federal prosecutor said November 8. The employee was arrested November 7 and charged with attempted extortion and the use of a destructive device. In an anonymous letter, the employee notified the manager of the Home Depot that he had placed a bomb there. The police were able to find it, took it away, and detonated it. But the employee's letter said he only wanted to prove he could plant a bomb without being detected. He then threatened to set off three more bombs at Home Depots on Long Island if he did not get the money, prosecution said. The letter said those bombs would shut down the stores on Black Friday. Each would hold a pound of roofing nails, according to the complaint. After a second letter was sent, lowering the ransom demand to \$1 million and setting a drop date for October 26, investigators were able to identify and arrest the employee. Source:

[http://www.salon.com/2012/11/08/feds\\_ny\\_man\\_planted\\_home\\_depot\\_bomb\\_to\\_extort\\_2m/](http://www.salon.com/2012/11/08/feds_ny_man_planted_home_depot_bomb_to_extort_2m/)

## **COMMUNICATIONS SECTOR**

**Skype security issue prompts password reset shutdown.** Skype, a tool that roughly 250 million users rely on for cheap, seamless international audio and video calling, suffered a security breach that could allow anyone to change a user's password and take over their account, PC Magazine reported November 14. According to reports, the simple hack can be executed as long as the intruder knows the user's account name and associated email address. In response, Skype has temporarily disabled the password reset feature in Skype to protect users. Originally discovered on a Russian hacker Web site, the exploit was tested and confirmed by TheNextWeb over the last 24 hours. Source: <http://www.pcmag.com/article2/0,2817,2412100,00.asp>

## **CRITICAL MANUFACTURING**

**Kawasaki Motors recalls fuel filters for lawn mower and utility vehicle engines due to fire hazard.** The U.S. Consumer Product Safety Commission, in cooperation with Kawasaki Motors Corp. USA, November 15 announced a voluntary recall of about 55,000 fuel filters and about 1,200 tune-up kits. The fuel filter can leak, posing a fire hazard. Kawasaki received 110 reports of fuel leaks in lawn mowers, including two reports of leaks from replacement filters. The filters and kits were sold at Kawasaki dealers nationwide between August 2011 and August 2012. Consumers should immediately stop using products with the recalled fuel filters and contact Kawasaki or a Kawasaki dealer for a free repair. Source:

<http://www.cpsc.gov/cpscpub/prerel/prhtml13/13041.html>

**Toyota to recall 2.8 million vehicles for steering glitch.** Toyota Motor Corp said it will recall 2.77 million vehicles worldwide for steering and water pump problems, Reuters reported November 14. Toyota said the defects had caused no accidents and could each be fixed in an

## UNCLASSIFIED

hour or so. The first recall covers 2.67 million 2000-2006 Corolla vehicles worldwide, 670,000 in the U.S., to fix a steering component that could be damaged by wear and tear. The other concerns 630,000 2004-2011 gasoline-electric hybrid Prius vehicles worldwide to replace water pumps, a company spokesman said. Many vehicles are targeted by both recalls, resulting in overlap. Source: <http://www.chicagotribune.com/classified/automotive/sns-rt-us-toyota-recall-priusbre8ad09a-20121113,0,3068364.story>

**LG Electronics recalls electric ranges due to burn and fire hazards.** The U.S. Consumer Product Safety Commission, in cooperation with LG Electronics, November 8 announced a voluntary recall of about 161,000 LG Electric Ranges. Burners on the electric ranges can fail to turn off after being switched off and the temperature setting can increase unexpectedly during use, posing burn and fire hazards to consumers. LG has received 80 reports of incidents involving burners failing to turn off or the temperature setting increasing unexpectedly during use. The units were sold at Best Buy, Home Depot, Sears, and regional appliance retailers nationwide from January 2006 to June 2010. Consumers should immediately contact LG to schedule a free in-home repair. Consumers whose burner heat setting cannot be regulated by using the controls or who experience problems with a cooktop burner remaining on, should immediately stop using the recalled electric range until it is repaired. Source: <http://www.cpsc.gov/cpscpub/prerel/prhtml13/13031.html>

**NHTSA recall notice - Jeep Grand Cherokee and Liberty air bag control module.** Chrysler announced a recall November 9 of 744,822 model year 2002 and 2003 Jeep Liberty vehicles manufactured from January 9, 2001 through March 28, 2003, and 2002 through 2004 Jeep Grand Cherokee vehicles manufactured from February 13, 2001 through May 23, 2003. A component in the air bag control module may fail causing the front airbags, side curtain airbags, and/or seatbelt pretensioners to deploy inadvertently while the vehicle is being operated. Inadvertent deployment of the airbags may increase the risk of injury and the possibility of a vehicle crash. Chrysler will notify owners, and dealers will install a supplemental jumper harness to the airbag control module, free of charge. The recall is expected to begin during January 2013. Source: [http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl\\_ID=12V527000&summary=true&prod\\_id=203408&PrintVersion=YES+](http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V527000&summary=true&prod_id=203408&PrintVersion=YES+)

## **DEFENSE/ INDUSTRY BASE SECTOR**

**Lockheed says cyber-attacks up sharply, suppliers targeted.** November 12, the U.S. Department of Defense's number-one supplier, Lockheed Martin, cited dramatic growth in the number and sophistication of international cyberattacks on its networks and said it was contacting suppliers to help them bolster their security. The company's vice president and chief information security officer said about 20 percent of the threats directed at Lockheed networks were considered "advanced persistent threats," prolonged and targeted attacks by a nation state or other group trying to steal data or harm operations. She said the company had seen "very successful" attacks against a number of the its suppliers, and was focusing heavily on

UNCLASSIFIED

## UNCLASSIFIED

helping those companies improve their security. Source:

<http://www.reuters.com/article/2012/11/13/net-us-lockheed-cyberidUSBRE8AC02S20121113>

### **EMERGENCY SERVICES**

**(Virginia) After derecho 911 outage, public safety officials promote landlines.** Verizon Wireless and local public safety officials presented a preliminary report to the Metropolitan Washington Council of Governments November 14 on the summer of 2012 derecho storm that resulted in a massive 9-1-1 outage of Verizon's 9-1-1 service across much of Northern Virginia.

Verizon blames the failure on one of two backup generators in its Arlington and Fairfax offices. Company officials said they are doing a better job communicating with 9-1-1 centers, and they are applying lessons learned. Public safety officials recommended more action by legislative bodies and regulatory bodies, like the Federal Communications Commission, to ensure each mobile carrier's 9-1-1 infrastructure and backup systems are fully functional through comprehensive audits. Source: <http://www.wjla.com/articles/2012/11/after-derecho-911-outage-public-safetyofficials-promote-landlines-82102.html>

**(Missouri) Emergency response times to be released following fierce scrutiny.** For months, emergency response times were under fire in Kansas City, Missouri. November 13, the interim fire chief was expected to release district-by-district response times to the Public Safety Committee. The amount of time it should take for an ambulance to arrive at the scene of an emergency is 9 minutes or less. However, recent statistics show ambulances arriving at a scene within that time frame at only 75 percent of the time. Due to a protocol change in December 2011, requiring dispatchers to get additional information from callers, ambulance response times have slowed by about minute. Fire officials said another reason for slower response time is that the number of emergency calls they have received over the past couple years doubled. Source: <http://fox4kc.com/2012/11/14/emergency-response-times-to-be-released-following-fierce-scrutiny/>

### **ENERGY**

**Report: Fifty-eight percent of Energy computers went months without bug fixes.** An internal audit found nearly 60 percent of Energy Department desktop computers were missing critical software patches. Officials risk disrupting agency business by applying patches because fixes likely would require pausing widely used programs, said the chief executive officer of EnergySec, a federally funded public-private partnership. The inspector general audit, which was released the week of November 12, covered unclassified systems at administrative offices department-wide. The assessment revealed that many desktops and servers were running without security patches. About 58 percent of the Energy desktops tested used operating systems or software without fixes for weaknesses that had been discovered, in some cases, up to six months earlier. Also, 41 network servers were running operating systems no longer supported by their developers. The probe was conducted between February and November and examined facilities overseen by the undersecretary for nuclear security, undersecretary of energy, and undersecretary for science. In a November 5 response to a draft report, the Energy

UNCLASSIFIED

## UNCLASSIFIED

chief information officer agreed to follow up on the uncovered problems. Source:

<http://www.nextgov.com/cybersecurity/2012/11/report-fifty-eight-percent-energy-computers-went-months-without-bug-fixes/59559/>

**Report warns electricity grid vulnerable to attack.** The electrical grid is vulnerable to terrorist attacks, including cyber strikes, that could cause far more damage than those associated with natural disasters such as Hurricane Sandy, according to a report released November 14. Without urgent attention to security, the United States risks having large parts of the country blacked out “for weeks or months” at a cost of billions of dollars, the National Research Council said. “Major cascading blackouts in the U.S. Southwest in 2011, and in India in 2012, underscore the need for the measures discussed in this report,” the group said. In the intervening 5 years, the potential for cyber attacks on critical elements of the electric power delivery system — including communications, sensors and controls, or other key infrastructure — has risen sharply. “Any telecommunication link that is even partially outside the control of the system operators could be an insecure pathway into operations and a threat to the grid,” the report said. The sprawling power transmission system, spread across hundreds of miles and with many key facilities unguarded, is “inherently vulnerable,” according to the council. Deregulation in the mid-1990s, designed to increase competition in the supply of bulk power, was said to have put the network even more at risk. As a result, many parts of the bulk high-voltage system are heavily stressed and at risk for multiple failures should an attack occur. Source:

<http://www.reuters.com/article/2012/11/14/us-usa-electricity-attacksidUSBRE8AD1LL20121114>

**Stuxnet infected Chevron’s IT network.** Stuxnet infected Chevron’s network in 2010, shortly after it escaped from its intended target, the Wall Street Journal reported November 13. Chevron found Stuxnet in its systems after the malware was first reported in July 2010, said the general manager of the earth sciences department at Chevron. Chevron was not adversely affected by Stuxnet, said a Chevron spokesman. Chevron’s experience with Stuxnet appears to be the result of the unintentional (and perhaps, inevitable) release of malware upon a larger network, much like an experimental virus escaping from a medical lab. Chevron is the first U.S. company to acknowledge that its systems were infected by Stuxnet, although most security experts believe the vast majority of hacking incidents go unreported for reasons of security or to avoid embarrassment. The devices used in industrial equipment and targeted by Stuxnet are made by huge companies, including Siemens. Source:

<http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/>

**(Idaho) Thieves steal \$25K in copper wire from site.** A construction company said thieves stole more than \$25,000 in copper wire from an Elmore County, Idaho construction site. Western Construction employees discovered the industrial cable used to run heavy equipment was missing November 12 from the site near Interstate 84. Western Construction estimated replacing the wire and repairing damage to equipment will cost \$50,000. The company is offering a \$5,000 reward for information that leads to an arrest.

Source: <http://www.newstimes.com/news/crime/article/Thieves-steal-25K-in-copper-wire-from-site-4032608.php>

UNCLASSIFIED

## **FOOD AND AGRICULTURE**

**Nestlé USA announces voluntary recall of NESQUIK Chocolate Powder.** Nestlé USA announced November 8 a voluntary recall of limited quantities of Nestlé NESQUIK Chocolate Powder in the 10.9, 21.8, and 40.7-ounce canisters, reported the U.S. Food and Drug Administration. The NESQUIK recall was the result of a calcium carbonate recall from supplier Omya, Inc. due to the possible presence of Salmonella. The products were distributed nationally, and have a best before date of October 2014. Source: <http://www.fda.gov/Safety/Recalls/ucm327533.htm>

## **GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)**

**(Indiana) Mailed-in bomb threat clears county courthouse.** An Anderson, Indiana woman was arrested November 15 in connection with a November 14 bomb threat at the Madison County Government Center. He said sheriff's detectives worked to follow up on leads and conducted interviews on the letter that was sent to the government center containing a bomb threat. A commotion started in the commissioners' outer office, with several people reading a letter addressed to Madison County Courts. The letter, which first went to the Madison County Council of Governments, contained a bomb threat and angry comments directed at a prosecutor and other officials, according to several people who read it. All three commissioners took the threat seriously. They called the sheriff and then ordered the immediate evacuation of the building. The County Human Resources Director said that 350 to 400 employees work in the building every day and that as many as 1,000 people transact there. The sheriff brought in his department's bombsniffing dog, and the Delaware County Sheriff's Department's bomb squad and dog assisted in the search. No explosive device was found, and employees returned to the building after a wait of about two hours. In addition, the Madison County Emergency Management Agency diverted traffic for a one-block area around the government center during the event. Source: <http://heraldbulletin.com/crime/x532283665/Mailed-in-bomb-threat-clearscounty-Courthouse>

**Mexican police commander linked to attack on U.S. Embassy vehicle.** A Mexican federal police commander was arrested and charged with providing false information in the case of 14 officers accused of ambushing a U.S. Embassy vehicle in August, authorities said November 13. Initial reports on the shooting, which wounded two CIA agents, said federal police mistook the embassy SUV for a criminal vehicle, but officials later said it appeared to be an intentional attack and raised the possibility it was staged at the behest of a drug cartel. The inspector general was jailed November 12, accused of lying to authorities about what happened in the August 24 attack south of Mexico City, two government officials familiar with the case said. The 14 officers, who were formally charged with attempted murder last week, were in plain clothes and civilian vehicles when they chased and fired at the gray Toyota SUV with diplomatic plates,

## UNCLASSIFIED

then peppered the windows of the armored vehicle with 152 bullets when it came to a stop. Two CIA officers, whose identities have not been released by the U.S. government, had non-life-threatening injuries, and a third person in the car, a Mexican navy captain, was not hurt. The officers so far do not face organized crime charges. However, the Mexican attorney general's office has said the investigation is continuing, and it is still exploring whether the officers had links with organized crime. Source: [http://www.thereporter.com/news/ci\\_21992983/mexican-police-commander-linked-attack-u-s-embassy](http://www.thereporter.com/news/ci_21992983/mexican-police-commander-linked-attack-u-s-embassy)

### **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**PoC malware for remote hijacking of USB smart readers.** Researchers from malware.lu have created proof-of-concept malware that allows attackers to gain access to and remotely control users' USB smart card readers. Smart cards (chip cards) are used for various purposes, among which are also user identification and authentication. Spanish and Belgian citizens already have an eID card that is used for identification, authentication, and for digital signing. Banks issue smart cards to customers who have opted for 2-factor authentication when accessing their online banking service, and many companies give them out to employees in order for them to be able to authenticate themselves when accessing the corporate network from a remote location. The malware works by installing on the victims' computer a special driver that shares the USB reader over TCP/IP, and another driver on the attacker's computer is able to translate that signal and make it look like the device is physically attached to his computer, Computerworld reports. The malware also has a keylogger component, making it possible for attackers to harvest any of the PINs or passwords that are used with the cards if the reader does not have its own keypad. Another current limitation of the malware is that the driver is not digitally signed and some OS will not accept unsigned software. Source: [http://www.netsecurity.org/malware\\_news.php?id=2325&utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:+HelpNetSecurity+\(Help+Net+Security\)&utm\\_content=Google+Reader](http://www.netsecurity.org/malware_news.php?id=2325&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader)

**Most organizations unprepared for DDoS attacks, study says.** Organizations are becoming increasingly concerned about system availability as they experience more and more distributed denial-of-service (DDoS) attacks, a new study said. The study, conducted by the Ponemon Institute, surveyed 705 IT security professionals on issues related to downtime and DDoS. While security pros have traditionally been focused on preventing data theft or corruption, today's professionals are more worried about system availability, the study says. "DDoS attacks cost companies 3.5 million dollars every year," Ponemon says. "Sixtyfive percent reported experiencing an average of three DDoS attacks in the past 12 months, with an average downtime of 54 minutes per attack." Most organizations do not have the ability to strike back at attackers. "While 60 percent say they want technology that slows down or even halts an attacker's computer, the majority (63 percent) of respondents give their organizations an average or below average rating when it comes to their ability to launch counter measures," the report states. Threequarters of organizations still rely on antivirus and anti-malware to protect themselves from attacks. Source:

## UNCLASSIFIED

## UNCLASSIFIED

<http://www.darkreading.com/riskmanagement/167901115/security/vulnerabilities/240142111/most-organizationsunprepared-for-ddos-attacks-study-says.html>

**Intel Corporation: McAfee Threats Report shows global expansion of cybercrime.** McAfee November 14 released the McAfee Threats Report: Third Quarter 2012, which explores techniques in cybercrime as well as the global evolution of cyber exploits. The latest report uncovers new details of "Operation High Roller." It states that mobile malware almost doubled the previous quarter's total, and reveals an all-time high in database breaches. McAfee Labs also saw jumps in some categories of malware, including ransomware and signed binaries. Rootkits and Mac malware continue to rise, while password-stealing Trojans and AutoRun malware also trended strongly upward. Source: <http://www.4-traders.com/INTEL-CORPORATION-4829/news/Intel-Corporation-McAfee-Threats-Report-Shows-Global-Expansion-of-Cybercrime-15509039/>

**Malware uses social media and blogging sites as part of its C&C server.** Researchers have uncovered some interesting phishing attacks that rely on blogging and social media Web sites as part of the command and control (C&C) server, Softpedia reported November 14. According to FireEye experts, it all starts with an attachment called "AutoCleanTool.rar." When the file is unzipped and executed, users are presented with a small application window which prompts them to enter their full email address and its associated password. Once the credentials are handed over, the information is saved into the Windows registry, after which it is transmitted to the attackers by the malware. In the meantime, a directory structure is created and a malicious DLL file is dropped in a couple of locations. Once the DLL (NetCCxx.dll) is loaded, the malware first checks to see if it can connect to the Internet by using a GET request. Then, it starts contacting a number of domains, all of which appear to be hosted on Chinese social media and blogging Web sites. From these Web sites, the malware starts downloading a series of .jpg image files. The images contain an "unknown padding," 471 bytes in size, after the "Endofimage" marker. This "unknown padding" is referenced by the threat in order to update itself. The data it takes from one image becomes part of a new .ini file that contains configuration details. Another part of the retrieved data contains the URL for an additional image file, which in turn contains more configuration information. This way, the malware can update itself without being noticed by security software. Furthermore, the data from the .jpg file can also be utilized to update the entire framework and even add new components. Source: <http://news.softpedia.com/news/Malware-Uses-Social-Media-and-Blogging-Sites-as-Part-of-Its-C-C-Server-306801.shtml>

**Researcher tracks down compromised ICS systems.** Supervisory control and data acquisition (SCADA) and industrial control systems' (ICS) security has been repeatedly questioned in recent months. Now, one researcher shows how easy it is to find ICS systems that have already been compromised, while another warns Siemens that just fixing SCADA vulnerabilities is an ongoing process, not a solution. In two Digital Bond posts the week of November 5, a researcher describes the SCADA vulnerability problem, and then a second researcher demonstrates how to locate such systems that have already been compromised. He concentrates on one particular

UNCLASSIFIED

## UNCLASSIFIED

system he found, “an extremely detailed DDS log.” “First off,” he writes, “this system has the SEL AcSELeRator Quickset and GE Enervista, so it was used to either review relay configurations or install relay configurations on SEL and GE digital protective relays.” In other words, it effectively plugs into the national power grid. “This suggests a technician’s laptop, one who works on a wide variety of electric power systems and other automation systems.” However, the laptop was infected with two pieces of malware: The fake antivirus and backup program “Malware Protection Designed to Protect” and “Windows XP Recovery.” Such malware is usually installed either by drive-by downloading or direct installation. Source:

<http://www.infosecurity-magazine.com/view/29267/researcher-tracks-downcompromised-ics-stems/>

**One in four users at risk due to outdated browsers.** Nearly a quarter of users do not use the latest browser versions, and those using Mozilla Firefox are the slowest when it comes to updating, which leaves them open to Web-based attacks, Kaspersky Lab warns. Basing their results on the information collected from their 10 million randomly selected customers from different regions across the world, the company discovered that Chrome users are nearly as numerous as Internet Explorer (IE) ones (36.5 and 37.8 percent, respectively), while the numbers for Firefox (19.5 percent) keep falling. While the news is not good for Mozilla, it is for security, as only 69.5 percent of Firefox users use the latest two versions, but 94.7 percent of Chrome users and 96.5 percent of IE users do the same. Also, compared to Chrome users, Firefox users update to the newer version at a slower speed and more users tend to stay on the older version for a longer period of time. The research differentiates between older (but still supported) versions of the browsers and the outdated ones, but still point out that 23 percent of the users have not opted for the latest versions and the security improvement they bring.

Source: <http://www.net-security.org/secworld.php?id=13934>

**Mushrooming ransomware now extorts \$5 million a year.** Malware that disables computers and demands that hefty cash payments be paid to purported law-enforcement agencies before the machines are restored is extorting as much as \$5 million from end-user victims, researchers said. The estimate, contained in a report published November 8 by researchers from antivirus provider Symantec, is being fueled by the mushrooming growth of so-called ransomware. Once infected, computers become unusable and often display logos of local law-enforcement agencies, along with warnings that the user has violated statutes involving child pornography or other serious offenses. The warnings then offer to unlock the computers if users pay a fine as high as \$200 within 72 hours. The report identified at least 16 different ransomware versions spawned by competing malware gangs. Many are completely different families of malware, rather than multiple variants of the same family, and most have their own unique behavior.

Source: <http://arstechnica.com/security/2012/11/mushrooming-growth-of-ransomware-extorts-5-million-a-year/>

**Experts find DOM-based XSS vulnerability in Google.com.** Security researchers from Minded Security identified a document object model (DOM)-based cross-site scripting (XSS) vulnerability on Google.com. The security hole was identified with the aid of DOMinatorPro — a runtime JavaScript DOM XSS analyzer. According to the researchers, DOMinatorPro revealed a

## UNCLASSIFIED

## UNCLASSIFIED

piece of code in googleadservices.com /pagead/landing.js which used invalidated input to build the argument for two "document.write " calls. They found that the buggy JavaScript was utilized by google.com/toolbar/ie/index.html (both HTTP and HTTPS). "[This] means that one more time a (almost) 3rd party script introduces a flaw in the context of an unaware domain," a researcher from Minded Security explained. He suggested a workaround, but Google decided to address this issue by removing the problematic script altogether. Source:

<http://news.softpedia.com/news/Experts-Find-DOM-Based-XSS-Vulnerability-in-Google-com-305585.shtml>

### **NATIONAL MONUMENTS AND ICONS**

Nothing Significant to Report

### **POSTAL AND SHIPPING**

**FedEx, UPS are targets of federal criminal investigation of shipments for online pharmacies.**

FedEx and UPS have disclosed they are targets of a federal criminal investigation related to their dealings with online pharmacies, which are at the center of an international crackdown on prescription drug abuse, the Associated Press reported November 15. The shipping companies made the disclosures in regulatory filings over the last several weeks. The investigation of the country's two largest shippers stems from a blitz against online pharmacies that was launched in 2005. A federal jury convicted three men of operating illegal pharmacies that used FedEx Corp. and UPS Inc. to deliver drugs without proper prescriptions. Seven others have been convicted in San Francisco in 2012. Both companies said they were served with grand jury subpoenas between 2007 and 2009. FedEx spokesman confirmed that the company is under investigation for allegedly aiding and abetting online pharmacies that illegally ship prescription drugs. Source: <http://www.foxnews.com/us/2012/11/15/fedex-ups-are-targets-federalcriminal-investigation-shipments-for-online/>

### **PUBLIC HEALTH**

Nothing Significant to Report

### **TRANSPORTATION**

Nothing Significant to Report

### **WATER AND DAMS**

**(Virginia) Contamination levels remain high after Sandy, spill.** Water and oyster samples in the Nansemond and lower James rivers in Virginia continue to show elevated contamination levels two weeks after Hurricane Sandy, and a related sewage spill prompted the State to close those areas to shellfish harvesting, a health department official said November 13. The director of the Virginia Department of Health Division of Shellfish Sanitation said samples would be taken from

UNCLASSIFIED

## UNCLASSIFIED

the Nansemond, lower James, and Lynnhaven rivers November 13 and November 14, weather permitting. Meanwhile, the Hampton Roads Sanitation District (HRSD) said it has taken steps to boost oxygen levels and speed the recovery of Shingle Creek, the site of a massive sewage spill. A spokeswoman for HRSD said workers began November 13 to pull water from the creek, saturate it with oxygen, and return it to the creek. The director of the Virginia Department of Health Division of Shellfish Sanitation said most of the lower Chesapeake Bay, from the Poquoson River south, was closed to shellfish harvesting in the storm's wake because of high levels of coliphage, a virus that indicates the presence of human pathogens associated with sewage contamination. Source: <http://hamptonroads.com/2012/11/contamination-levels-remain-high-after-sandy-spill>

**Deadly 'superbug' found in water treatment plants.** Researchers from the University of Maryland and the University of Nebraska Medical Center found that at least four water treatment plants in the United States contain superbugs, the methicillin-resistant *Staphylococcus aureus* (MRSA) and the methicillin-susceptible *Staphylococcus aureus*, Medical Daily reported November 8. The concern is that the plants are putting sewage workers at risk for contracting the bacteria, and that plants that do not treat water with chlorine may be leaving the most lethal strains. The four treatment plants in the Mid-Atlantic and the Midwest were treated effluent, in which wastewater with solids and some other impure substances, is used to irrigate and fertilize fields. The researchers wanted to discover whether MRSA could be spreading in that manner. The researchers found that 83 percent of the sewage in the plant was infected with the bacteria, and that 93 percent of MRSA was resistant to two or more antibiotics. However, as the treatment process continued, the number of bacteria declined. Only one plant had MRSA still alive at the end of the process; this one did not regularly chlorinate the water at their facility. The study was published in the journal *Environmental Health Perspectives*. Source: <http://www.medicaldaily.com/articles/13008/20121108/deadly-superbug-found-water-treatment-plants.htm>

## **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](mailto: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](mailto:kihagel@nd.gov), 701-328-8168

UNCLASSIFIED