



Department of Homeland Security Daily Open Source Infrastructure Report for 27 March 2007

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- The Federal Aviation Administration announced last week that a new way of handling air traffic in and around New York, New Jersey and Philadelphia will help reduce delays and make air travel more reliable. (See item [11](#))
- The Associated Press reports that the Transportation Security Administration is among several policing agencies that started boosting the law enforcement presence in New York on the Metro–North Railroad, the Long Island Rail Road and the Staten Island Railway last week. (See item [13](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *March 25, Los Angeles Times* — **Refinery breakdowns on rise.** Refineries across the country are breaking down with unusual frequency this year, boosting prices at the pump and endangering workers and communities. The rash of oil plant problems may not be a coincidence. The breakdowns stem from the hard use of aging equipment, a shortage of trained workers, corporate cost-cutting and ownership changes, refinery experts say. In the first six weeks of 2007, there were 43 incidents involving pipeline leaks, chemical releases, plant breakdowns and fires, more than has been typical, Kim Nibarger, a safety expert for the United

Steelworkers Union, told Congress during a hearing last week on refinery safety. Several of the accidents left employees injured. The incidents, coupled with an abnormal number of maintenance projects and mishaps, recently pushed the average per-gallon cost of gasoline higher. "Refineries are potentially dangerous places, but they can be managed in a more safe manner," said Dave Campbell, secretary-treasurer of the steelworkers local that represents refinery workers in Southern California. Campbell said tighter regulation and greater government scrutiny made California refineries safer than others, but he added that those safeguards could be undermined by budget cutting, production demands and other pressures. Source: <http://www.sun-sentinel.com/business/local/sfl-sboil25mar25.0.1712151.story?coll=sfla-business-headlines>

2. *March 25, News Journal Online (FL)* — **Demand for copper spurs costly, and dangerous, thefts.** The New Smyrna Beach, FL Utilities Commission has been victimized by copper thefts at least eight times since January. In most cases, the thieves cut fences to take spools of wire from storage areas, but last week someone cut the ground wiring from an active substation west of Interstate 95 and knocked out power to about 2,000 customers. Tim Beyrle, the utilities' director of system operations and generation, estimates the thefts have cost the utility 300 to 400 feet of cable, with a scrap value of between \$1,000 and \$1,200, but that doesn't include the cost of repairing any damage. Two Florida Power & Light (FPL) substations were hit last week near the Spruce Creek Fly-In. FPL spokesperson Bob Coleman said the Spruce Creek substation thefts were the first of their kind in his 16 years with the company. Progress Energy spokesperson C.J. Drake said there have been incidents at his company's substations in other parts of the state, including three in Polk and Orange counties in recent weeks. "It is an intermittent problem," he said, adding the substation thefts cost the company \$70,000 for repairs and restoration. Source: <http://www.news-journalonline.com/NewsJournalOnline/News/Headlines/frtHEAD05032507.htm>

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

3. *March 26, Hartford Courant (CT)* — **Explosion at gas station prompts road closure.** Gasoline spilling from a ruptured gas pump on Park Street ignited early Monday morning, March 26, causing an explosion at the gas station and a secondary explosion at a neighboring business in Hartford, CT. Firefighters and police officers, investigating a pickup truck that had rolled into the pump, were at the 7 Eleven during the explosion at 2 a.m. EDT. No one was injured. A section of Park Street at Prospect Avenue was closed. Fire officials are trying to determine why the pump's safety system didn't automatically kick in to stop gas from flowing. Deputy Chief Michael Ciccarelli said the fire department was called shortly after 2 a.m. after a pickup truck rolled into a gas pump, causing gasoline to spill. Vapors from the gasoline seeped into a neighboring doughnut shop and exploded when the business' gas burner kicked in, he said. Source: <http://fox61.trb.com/news/hc-hfdexplode-0326.0.5149351.story?coll=wtic-news-3>
4. *March 25, NewsNet5 (OH)* — **Chemical spill prompts evacuation.** Residents in Newburgh Heights, OH, returned home after a chemical spill Saturday, March 24. The nitric acid spill

happened at McGean Chemical on Harvard Avenue in Cuyahoga Heights. The gas traveled toward Newburgh Heights, forcing about 100 people from their homes to City Hall.

Source: <http://www.newsnet5.com/news/11372386/detail.html>

5. *March 24, Santa Rosa Press Democrat (CA)* — **Toxic fumes prompt students to remain indoors.** Toxic fumes were released from an oil refinery in Torrance, CA, but nobody was injured, authorities said. Hydrogen sulfide and sulfur dioxide were released into flares at the ExxonMobil Torrance Refinery after the plant south of Los Angeles had a problem with its sulfur recovery unit and shut down Thursday, March 22. The gas level at the ground did not pose a health hazard. However, students at nearby schools were kept indoors as a precaution for about three hours.

Source: <http://www1.pressdemocrat.com/apps/pbcs.dll/article?AID=/20070324/NEWS/703240336/1033/NEWS01>

[\[Return to top\]](#)

Defense Industrial Base Sector

6. *March 26, Government Accountability Office* — **GAO-07-640R: Defense Services Acquisition: Questions for the Record (Correspondence).** On January 17, Katherine V. Schinasi, the Government Accountability Office's (GAO) Managing Director of Acquisition and Sourcing Management testified before the Subcommittee on the Department of Defense's (DoD) management of its acquisition of services. Schinasi made several key points during the hearing. First, DoD's long-standing problems with contract management have become more prominent as DoD's reliance on contractors to provide services continues to grow. Second, DoD lacks sound contracting practices when acquiring services. Third, DoD's acquisition workforce has been downsized without sufficient attention to requisite skills and competencies. Fourth, DoD's acquisitions have resulted in outcomes that have cost the department valuable resources. And, finally, while DoD is taking some steps to address these problems, it does not know how well its services acquisition processes are working, which part of its mission can best be met through buying services, and whether it is obtaining the services it needs while protecting DoD's and the taxpayer's interests. Within this context, members of the Subcommittee requested that GAO provide additional comments on DoD's efforts regarding the following topics: interagency contracting, acquisition of services, acquisition reform, and the acquisition workforce. The questions and GAO's answers are provided in appendix I.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-640R>

[\[Return to top\]](#)

Banking and Finance Sector

7. *March 26, Associated Press* — **U.S. treasury officials, Chinese discuss frozen North Korea funds.** A senior Department of the Treasury official and Chinese officials tried Monday, March 26, to untangle a dispute over frozen North Korean funds that led to a breakdown in talks over the country's nuclear program. Daniel Glaser, deputy assistant secretary for terrorist financing and financial crimes, met Chinese foreign ministry and banking officials to discuss the money

held at Banco Delta Asia, a lender in the Chinese territory of Macau, the U.S. said. North Korea walked out of six-nation disarmament talks last week because of a hold-up in the release of the \$25 million. The U.S. agreed to let the money be transferred to a North Korean account at the Bank of China in Beijing, but the release was delayed by the Chinese bank's concerns about accepting money that had been linked to counterfeiting and money laundering. Glaser said in a statement before he left Washington that "the policy and diplomatic issues have been solved – this is now down to implementation."

Source: <http://www.signonsandiego.com/news/world/20070326-0521-korea-s-nuclear.html>

8. *March 26, SCMagazine* — **Phishing fraud emails target domain name owners.** Domain name owners are the target of a sophisticated scam disclosed by the SANS Internet Storm Center late last week. According to a report received by the nonprofit organization, scammers initially sent victims an email with an offer to purchase a domain name. Recipients were then directed to what appeared to be a forum discussion page addressing the most reliable appraisal services for domain names, according to SANS researcher Lenny Zeltser. The bogus email read, "Of course we must be sure that you are engaging a reputable appraisal company. I heard many appraisal companies often made inaccurate appraisals. I will only accept appraisals from independent sources I trust," and then links recipients to a forum page. Ron O'Brien, senior security analyst at Sophos said that the primary motivation of the scammer was to take \$99 payments while knowing the domain name won't be sold, although other motives are possible. Source: <http://scmagazine.com/us/news/article/646172/phishing-fraud-emails-target-domain-name-owners/>
9. *March 25, Computerworld* — **Microsoft acknowledges Xbox Live pretexting.** Months after Xbox Live users began complaining of hacked accounts, Microsoft Corp on Saturday, March 24, acknowledged that the service's support staff is at fault, victims of "pretexting" calls by identity thieves. Reports of account theft on Xbox Live have been making the rounds of its member forums since at least December. But Microsoft responded only after noted security researcher — Kevin Finisterre of "Month of Apple Bugs" fame — last week went public about how his account was hijacked. Larry Hryb, director of programming at Xbox Live, said they are examining the policies and have already begun retraining the support staff and partners to help make sure we reduce this type of social engineering attack. Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014218&intsrc=hm_list

[\[Return to top\]](#)

Transportation and Border Security Sector

10. *March 25, Associated Press* — **Smoke forces evacuation of El Al jet.** An El Al jet taxiing before takeoff at Ben Gurion International Airport near Tel Aviv, Israel, filled with smoke on Sunday, March 25, forcing passengers and crew to flee the aircraft on emergency slides, airport officials said. The 128 passengers and crew members on the Zurich-bound 737 were evacuated after smoke began billowing out of vents on the plane, airport spokesperson Yiftach Kramer said. No one was hurt in the mishap, the cause of which was still unknown, he said. Source: <http://www.forbes.com/feeds/ap/2007/03/25/ap3549074.html>

11. *March 23, Federal Aviation Administration* — FAA identifies new way to handle air traffic.

A new way of handling air traffic in and around New York, New Jersey and Philadelphia will help reduce delays and will make air travel more reliable, the Federal Aviation Administration (FAA) said Friday, March 23. After extensive analysis and public hearings in five states — New York, New Jersey, Pennsylvania, Delaware and Connecticut — the FAA has identified its preferred airspace redesign alternative for the New York area. That plan would combine high–altitude and low–altitude airspace to create more efficient arrival and departure routes. The preferred alternative is one of four proposals being studied. The plan, known as the Integrated Airspace Alternative, would reduce the complexity of the current air traffic system operation in the New York area and Philadelphia by more efficiently directing aircraft to and from major airports in the two metropolitan areas. The preferred alternative would save an estimated 12 million minutes of delay annually for the four major metropolitan airports — Kennedy, LaGuardia, Newark and Philadelphia.

Source: http://www.faa.gov/news/press_releases/news_story.cfm?newsId=8406

12. *March 23, Information Week* — FCC says 'no' to cell phones on airplanes, but Europe says 'yes'. While the Federal Communications Commission (FCC) is moving to kill the idea of cell phone service on commercial aircraft in the United States, European regulatory agencies remain positive on in–flight mobile phone calling. FCC Chairman Kevin Martin on Thursday, March 22, told reporters that his agency would give up looking into whether to approve the use of cell phones on airplanes. An opposite situation is under way in Europe, however, where regulatory agencies are working to pave the way for cell phone use on commercial aircraft. It's going through the approval process right now," said Charlie Pryor, a London–based spokesperson for OnAir, a planned mobile phone service sponsored by European aircraft manufacturer Airbus. According to Pryor, the Europeans have been testing their system for months and certification is being reviewed by the European Aviation Regulatory Authority. Another process involves the use of radio spectrum, being studied by the European Conference of Postal and Telecommunications Administrations (CEPT). CEPT has been working to coordinate some 44 European nations so they can allocate spectrum for mobile phone service providers. One of the FCC's concerns is the potential for cell phones on airplanes to disrupt other radio communications, according to the New York Times.

Source: <http://www.informationweek.com/news/showArticle.jhtml;jsessionid=CHL0H0E0R0ECSQSNDLPCKH0CJUNN2JVN?articleID=198500379>

13. *March 21, Associated Press* — TSA, New York state police join commuter rail security effort. The Transportation Security Administration is among several policing agencies that will boost the law enforcement presence in New York on the Metro–North Railroad, the Long Island Rail Road and the Staten Island Railway, the Metropolitan Transportation Authority announced Wednesday, March 21. "This combined deployment of MTA police and officers from a variety of federal and regional sources will give our commuter railroads the kind of police presence our customers deserve and the post–9/11 environment requires," said Elliot G. Sander, the MTA's executive director. Citing security concerns, officials would not say how many new officers would be patrolling the trains and platforms, but MTA spokesman Jeremy Soffin said the number would be "dramatically higher." The new security plan is called the Directed Patrol Strategy. It began last week with a new deployment plan for MTA officers and 50 dogs trained to sniff out explosives. Besides TSA marshals, passengers will see state police, county police from Westchester, Nassau, Suffolk and other counties and local police from

dozens of towns and villages, Soffin said. New York City police will take part at railroad stations in the Bronx, Queens and Staten Island. Officials said the new patrols could do random bag searches.

Source: <http://news.bostonherald.com/national/northeast/view.bg?articleid=189974>

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture Sector

14. *March 23, Agricultural Research Service* — Lettuces resist corky root, mosaic virus. Iceberg lettuce faces attack from an array of microbes that are deadly to the vegetable. That's why Agricultural Research Service (ARS) scientists developed seven kinds of parent iceberg lettuces that shrug off attack by two microbial enemies. One, a disease known as corky root, causes lettuce roots to develop ugly, yellow-to-brown lesions that harden to a corklike texture. Corky-root-infected plants may produce stunted heads 30 to 70 percent smaller than normal. The other headache, lettuce mosaic, is caused by a virus of the same name. It results in stunted growth as well as unattractive mottling of leaves. Green peach aphids, about one-eighth-inch long, can spread the virus from an infected plant to an uninfected one as they move about a lettuce field. The parent plants debuted in 2006 as the first publicly available crisphead lettuces — developed especially for California climates and soils — that come equipped with powerful natural resistance to both microbes.

Source: <http://www.ars.usda.gov/is/pr/2007/070323.htm>

[\[Return to top\]](#)

Food Sector

15. *March 26, Agence France-Presse* — Test could prevent food poisoning. Whether to dispose of food products or eat them is in many cases a judgement call, but researchers announced Sunday, March 25, that they have come up with a tool that could take the guesswork out of the decision-making process. The tool is a disposable dipstick that can detect whether a food is still safe to eat or whether it's a health hazard that could lead to a case of food poisoning. In laboratory tests, the device had a 90 percent accuracy rate. The dipstick is made of special polymers or synthetic materials that change colour in the presence of chemicals formed by disease-causing bacteria.

Source: http://news.yahoo.com/s/afp/20070326/hl_afp/ushealthfood_070_326122420

16. *March 24, Agence France-Presse* — Tainted pet food producer expands recall. The Canadian company that sold tainted pet food blamed for at least 14 pet deaths expanded its product recall Saturday, March 24, saying it worried consumers could still find the products on store shelves. Toronto-based Menu Foods said some of its pet foods, possibly tainted with a

toxin used as rat poison, were still being sold. The company said store owners should remove all of its products, regardless of the production date. Last week the Menu Foods recalled 60 million cans and pouches of food made in the U.S. and sold under 95 different brand names after reports that house pets were falling sick and dying after eating the some of their products. Source: http://www.breitbart.com/article.php?id=070324234604.hfiw5vn g&show_article=1

17. *March 24, Bloomberg News* — One source not found for E. coli in spinach. E. coli bacteria in bagged spinach that killed three people and sickened at least 205 last year could not be traced to a specific cause, U.S. regulators said Friday, March 23. Investigators from the U.S. Food and Drug Administration (FDA) and California Health Services Department found the bacteria in wild pigs, irrigation wells and surface waterways near four spinach farms, the agencies said in a conference call, but they were unable to figure out how it got into the food supply. Sales of leafy greens have fallen 30 percent this year on public fear of another outbreak, according to Western Growers, a trade group based in Irvine, CA. The FDA had said in October that cattle feces on one of the four ranches being investigated in Monterey and San Benito counties had the same bacteria strain as was found in the tainted spinach.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/03/23/AR2007032301733.html>

18. *March 24, U.S. Food and Drug Administration* — FDA warns again about arsenic in mineral water. The U.S. Food and Drug Administration (FDA) is re-issuing its warning to consumers not to drink "Jermuk" brand mineral water due to the risk of exposure to arsenic, a toxic substance and a known cause of cancer in humans. The agency is providing this information again to consumers due to an expansion of the recall initiated by the products' importers and distributors. "Jermuk" water is imported from Armenia and distributed under different labels in California. Five brands of these products have been recalled since March 7. The latest recall, which was initiated on March 16 by the product's distributor, Andreas Andreasyan DBA Arnaz & Nelli Co., North Hollywood, CA., is for "Jermuk Natural Mineral Water Fortified with Gas from the Spring". FDA has sampled the contents of 500 milliliter (mL) green glass and/or plastic bottles of all of these brands and found they contained 454–674 micrograms of arsenic per liter of water. FDA's standard of quality for bottled water allows no more than 10 micrograms per liter. The agency is investigating whether other bottle sizes or types of packaging contain similarly tainted products, and will continue working to remove all such bottled water from the market.

Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01594.html>

19. *March 23, U.S. Food and Drug Administration* — Dog treats recalled. Petrapport, Inc. is voluntarily recalling pig ear dog treats it imported from a Chilean company during the period August 2006 through December 2006 because the pig ears have the potential to be contaminated with Salmonella, an organism that can cause serious infections in dogs, and, if there is cross contamination, young children, frail or elderly people, and others with weakened immune systems. Laboratory testing has confirmed that samples of Full-Cut Pig Ears dog treats sold by BJ's Wholesale Club in 25-count packages under the "Berkley & Jensen" brand with no lot number were contaminated with Salmonella.

Source: http://www.fda.gov/oc/po/firmrecalls/petrapport03_07.html

[[Return to top](#)]

Water Sector

20. *March 24, Shanghai Daily (China)* — **Five million short of drinking water.** More than five million people are short of drinking water in China's southwestern province of Sichuan as a result of a worsening drought. Water shortages have affected 5.5 million people, 6.3 million livestock and 560,000 hectares of crop land across the province. In the worst-hit areas, residents are having their drinking water delivered to them by government trucks.

Source: http://www.shanghaidaily.com/sp/article/2007/200703/20070324/article_310200.htm

[\[Return to top\]](#)

Public Health Sector

21. *March 26, Reuters* — **Asian nations, World Health Organization meet over H5N1 sharing row.** Drawing up rules aimed at restricting how virus samples shared amongst countries are used would slow down global efforts to develop vaccines, the World Health Organization's (WHO) top bird flu official said on Monday, March 26. Indonesia, which is hosting a WHO meeting with health officials from 18 nations to discuss the issue, has said it will only share samples of the H5N1 avian influenza virus if it has guarantees they will not be used commercially. Jakarta has also said it wants WHO to help draw up "material transfer agreements" to control the use of samples. Some health and aid agencies have criticized Indonesia for refusing to share samples, while others defended the stance because developing countries often struggle to get access to life-saving drugs due to patent laws and high costs.

Source: <http://www.alertnet.org/thenews/newsdesk/JAK73717.htm>

22. *March 25, Agence France-Presse* — **Bird flu outbreak spreads in Bangladesh.** Three new farms reported bird flu outbreaks in Bangladesh Sunday, March 25, after thousands of poultry were destroyed last week due to confirmed cases of the deadly virus, the government said. On Friday, March 23, authorities slaughtered more than 40,000 birds at six farms, a day after official confirmation of a bird flu outbreak on the outskirts of Dhaka. The outbreak was now suspected to have spread to farms in the north and central parts of the country, government spokesperson Abdul Motalib said. "Today we have detected bird flu in three more farms in the northern district of Jamalpur and destroyed some 9,000 birds there. We will now destroy all the birds within a 0.6-mile area of the infected farms," he said. "We also have reports of mass deaths of chickens in central Narayanganj and northern Dinajpur districts. We have sent the samples to laboratories for tests," Motalib said.

Source: http://news.yahoo.com/s/afp/20070325/hl_afp/healthflubangladesh_070325211205;_ylt=Ap3a6F9CPIom9PJlcGk57miJOrgF

23. *March 24, Independent (South Africa)* — **World Health Organization to help with extremely drug resistant tuberculosis.** The World Health Organization (WHO) is sending an expert to South Africa to assist with extremely drug resistant tuberculosis (XDR-TB) — detected in 10 more people in the Eastern Cape, the provincial health department said on Saturday, March 24. The latest cases bring to 54 the number of people affected by the illness in the province since November 2006, said department spokesperson Sizwe Kupelo. Acting Health Minister Jeff

Radebe said the WHO official would arrive next week to give technical assistance, advice on training and the management of XDR–TB cases, infection control and improvement of surveillance system and laboratory services. The official would also conduct an epidemiological assessment of the number of cases that were reported in Tugela Ferry in KwaZulu–Natal last year.

Source: http://www.int.iol.co.za/index.php?set_id=1&click_id=125&art_id=nw20070324142633738C289138

[\[Return to top\]](#)

Government Sector

24. *March 26, Fox News* — Aide arrested for taking gun into Senate building. U.S. Capitol Police arrested a top aide to Senator Jim Webb on Monday, March 26, after he tried to enter a Senate office building carrying a loaded pistol and two fully loaded magazines that belonged to the senator. Phillip Thompson sent a bag through the X–ray machine at Russell Senate Office Building, where Webb's office is located. It detected the weapon and Capitol Police say they determined that Thompson didn't have a license to carry the gun in Washington, D.C. Handguns are illegal in Washington, D.C., but nearby Virginia allows residents to carry concealed handguns. Capitol Police rules allow members and their employees to bring a weapon onto Capitol grounds if it is unloaded and securely wrapped.

Source: <http://www.foxnews.com/story/0,2933,261368,00.html>

[\[Return to top\]](#)

Emergency Services Sector

25. *March 24, Salem–News (OR)* — Oregon Civil Air Patrol prepares for terrorist response training. The Oregon Wing of the Civil Air Patrol (CAP), in coordination with the United States Air Force and the Department of Homeland Security, will be participating in a week long six–state simulated terrorist training and evaluation exercise starting next weekend. The exercise, based on a simulated terrorist attack somewhere in the western United States, will utilize multiple bases of operations throughout the state where six Oregon CAP aircraft are assigned. The exercise will utilize a state headquarters Incident Command Post located at the Aurora State Airport. The scope of the exercise, which includes each of the six states in the CAP's Pacific Region — Oregon, Washington, California, Hawaii, Alaska, and Nevada — will involve a variety of simulated terrorist incidents in each state and will be used to evaluate the ability of CAP to respond to forecasted requests for assistance from state and Federal agencies responding to the incidents.

Source: http://www.salem–news.com/articles/march242007/cap_terrorism_32407.php

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

26.

March 26, Computerworld — **U.S.–based servers host majority of malicious code, study finds.** Forget China, Russia or eastern European countries. When it comes to malicious code, U.S.–based servers host an overwhelming majority of it, according to security vendor Finjan Inc. That conclusion is based on an analysis of more than 10 million URLs collected from live end–user traffic in the U.K. Each IP address was tracked to its exact geographical location, said Yuval Ben–Itzhak, chief technology officer at Finjan. The other top countries hosting malicious code are the U.K., with 10%, and Canada, Germany and Italy, Ben–Itzhak said. One of the reasons for the trend could simply be that free Web hosting servers are more readily available in North America and Europe than in some other regions, according to Finjan. That makes it more cost–effective for cybercriminals to host malicious code on servers in those countries. In many cases, malicious code also appears to have been hosted on servers offering legitimate content that were compromised by hackers, the report said.

Report: <http://www.finjan.com/Pressrelease.aspx?id=1383&PressLan=123 0&lan=3>

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014298&intsrc=hm_list

27. *March 26, CNET News.com* — **Windows weakness can lead to network traffic hijacks.** A problem in the way Windows PCs obtain network settings could let attackers hijack traffic, security researchers said Saturday, March 24, at the the ShmooCon hacker conference in Washington, DC. The problem occurs because of a design bug in the system used by Windows PCs to obtain proxy settings, researchers with security firm IOActive said. As a result, an attacker with access to a network at a corporation, for example, could insert a malicious proxy and see all the traffic. If an attack is successful, all traffic on a network will flow through the attacker's proxy. This means the attacker can access all the data, redirect and manipulate it and carry out all kinds of other nefarious acts, said Chris Paget, director of research and development at IOActive. Still, the proxy problem isn't a critical security issue. An attack is possible only with access to the target network, not from the Internet, they noted. "The biggest risk inside a corporation would come from a malicious insider," Paget said.

Microsoft acknowledged the problem in a support article published on its TechNet Website:

<http://support.microsoft.com/kb/934864>

Source: http://news.com.com/Windows+weakness+can+lead+to+network+traffic+hijacks/2100-1002_3-6170229.html?tag=cd.lede

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

28. *March 23, CNET News* — **A new day for business security.** It might not seem as if a building security guard and a network administrator have much in common. But they do — and the

distinction between the two is blurring more every day. It's true that the people who control building access from security desks and those securing computer networks both watch traffic and walk perimeters to safeguard an organization's assets. But now, technology, tighter security controls, federal regulations and potential cost benefits are bringing the two traditionally separate worlds together. The next two years will prove important in bringing together the security disciplines, observers say. Challenges include creating interoperability and making sure the one system that controls all aspects of security is safe from breaches. Unifying technologies include network-connected surveillance cameras and mechanisms to control building access that tie into the same systems used to grant network access. Software can catch what the human eye might not, such as somebody sneaking into a building behind another person who just swiped a security badge. Also, a single system for credentials can replace multiple access systems and passwords. One badge, or smart card, could be used to enter buildings, log on to networks and buy lunch in the campus cafeteria.

Source: http://news.com.com/A+new+day+for+business+security/2100-7355_3-6168256.html

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information: Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform

personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.