



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 16 March 2004

Current Nationwide Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Straits Times Asia reports that as Europe beefs up rail security after last week's deadly Madrid bombings, Britain will deploy anti-terror marshals on trains across the country and throughout London's underground network, among other measures. (See item [10](#))
- The New Straits Times says a report now out asserts that al Qaeda plans to disrupt the seaborne trading system, the backbone of the modern global economy, using a crude nuclear explosive device or a radiological bomb if possible. (See item [11](#))
- TechWeb News reports two new versions of the Bagle worm, Bagle.n and Bagle.o, were spotted over the weekend and unlike earlier editions of Bagle, the new Bagles may use a different archive format. (See item [24](#))
- Security Focus has raised ThreatCon to Level 2, citing a need for increased vigilance. Please refer to the Internet Alert Dashboard.

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

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

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

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

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

Other: [General](#); [DHS/IAIP Web 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://esisac.com>]

1. *March 12, Electric Light & Power* — Electric reliability and outage preparedness task force releases positive findings. Seven months after a cascading power outage swept through

northeastern United States and Canada, the Massachusetts Task Force on Electric Reliability and Outage Preparedness determined the Massachusetts electric infrastructure currently meets all reliability standards. The report notes, however, that the level of demand for electricity will change over time, as will the number and type of resources available to serve Massachusetts businesses and residents. Looking forward, the Task Force offers a comprehensive set of recommendations — twenty–six in total — to ensure that Massachusetts electric customers will continue to benefit from a stable, reliable electric system. **The thirty member Task Force was established by Governor Romney the day after the blackout to investigate the reliability of electric service in Massachusetts and to make recommendations to assess the Commonwealth's vulnerability to widespread or cascading power outages.** Several of the Task Force recommendations focus on preparedness – providing independent system operators with the necessary tools, information and training to respond to unexpected events of the type that triggered the August 14th blackouts. Report:

<http://www.state.ma.us/dpu>

Source: http://uaelp.pennnet.com/articles/article_display.cfm?Section=ONART&Category=INDUS&PUBLICATION_ID=22&ARTICLE_ID=200628

2. *March 11, San Gabriel Valley Tribune (CA)* — **Southern California blackout is not preview of summer problems, agency says.** Southern California likely will not experience rolling blackouts this summer, despite an "anomaly" that shut down power to about 70,000 energy customers in about 100 communities on Monday, March 8. "I don't think (Monday) says anything one way or the other about the coming summer months," said Gregg Fishman, a spokesperson for the California Independent System Operator, an agency that manages most of the state power grid. **More than 18 power plants have been built or completed since 2000, most able to produce 50 megawatts. "But we haven't seen the transmission grid keep up with that capacity," he added. That means there could be "choke points" in the transmission of power this summer, something that could cause a blackout just like on Monday.** When power use surged on Monday because of record high temperatures, one key transmission line that brought electricity into the region overloaded and had to be shut down, Fishman said. Officials say during the summer months they expect major strains on power systems but will not be caught off guard. "It was certainly unexpected," said Steve Conroy, spokesman for Southern California Edison.

Source: <http://powermarketers.net/contentinc.net/newsreader.asp?ppa=8knpp%5EZhlquwyz%5BTgd%216%3C%22bfej%5Bv>

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

3. *March 15, General Accounting Office* — **GAO–04–391: Tactical Aircraft: Changing Conditions Drive Need for New F/A–22 Business Case (Report).** Following a history of

increasing cost estimates to complete F/A–22 development, Congress asked the General Accounting Office (GAO) to assess the Air Force's F/A–22 development program annually and determine whether the Air Force is meeting key performance, schedule, and cost goals. On April 23, 2003, a congressional subcommittee requested that the Department of Defense (DoD) provide more detailed information on the business case that supports the estimated quantities and costs for an affordable F/A–22 program. Specifically, GAO (1) identified changes in the F/A–22 program since its inception, (2) reviewed the status of the development activities, and (3) examined the sufficiency of business case information provided for congressional oversight. GAO recommends that DoD complete a new business case that determines the continued need for the F/A–22 and the number of aircraft required for its air–to–air and air–to–ground roles based on capabilities, need, alternatives, and constraints of future defense spending departmentwide. Highlights:

<http://www.gao.gov/highlights/d04391high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-391>

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

Banking and Finance Sector

4. *March 14, Associated Press* — **Bomb found at U.S. bank in Athens.** Police used a controlled explosion Sunday, March 14, to neutralize a small time bomb planted outside an American bank office in Greece. There were no injuries or damage in the incident. **Police said the device, which included dynamite, was destroyed in two controlled explosions by its bomb squad outside a Citibank branch in the northeastern Athens suburb of Halandri.** Authorities had been alerted to the bomb by an anonymous telephone call to an Athens newspaper. There was no immediate claim of responsibility, but the attempt was thought to be the work of one of the many self–proclaimed anarchist groups and arson gangs that have in the past targeted banks. They have also targeted various businesses and diplomatic vehicles. Their favored targets are automatic teller machines at banks.

Source: <http://edition.cnn.com/2004/WORLD/europe/03/14/greece.bomb.a.p/index.html>

5. *March 12, Reuters* — **BJ's Wholesale consumer info may have been stolen. BJ's Wholesale Club Inc. said on Friday, March 12, its computer system may have been compromised and it has alerted its members that their credit card information may have been stolen.** The Natick, MA, warehouse club operator said in a statement it recently learned that a small fraction of its 8 million members may have been affected. The company said it has notified police and was working with credit card companies. BJ's said it conducted a review of its technology systems with a computer security firm and does not believe there was a central break–in of its systems.

Source: <http://cbs.marketwatch.com/tools/quotes/newsarticle.asp?symb=&guid=%7BA9ABD245-E058-4FA1-903C-2B8109A44974%7D&siteid=google&dist=google>

6. *March 10, MSNBC* — **The meth connection to identity theft. It is a twin–headed monster ravaging communities across the nation: methamphetamine addiction and identity theft. Police officers around the country say nearly every time they bust an ID theft ring, the criminals are meth addicts.** The drugs and the crime fit neatly together; addicts strung out on

meth can stay awake and focused for days at a time, making them expert hackers and mailbox thieves. ID theft is easy money, the perfect income for drug addicts who have no other way to fund their habit. Last year, police busted 9,300 meth labs, and the Federal Trade Commission says 10 million consumers were victims of ID theft. It's not clear which came first, the addiction, or the criminal explosion, but **increasingly, authorities believe the struggle against meth use and fight against ID theft are largely the same battle.** "Ninety percent of our ID theft cases deal with drugs," said Eugene, OR, police detective Steve Williams. And it's usually methamphetamine, which is easy and cheap to produce in mass quantities, said Williams. Source: <http://msnbc.msn.com/id/4460349/>

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

Transportation Sector

7. *March 15, Miami Herald* — **New York City mayor downplays fears of terrorist attack on city subways.** Mayor Bloomberg said the city's subway system was safe from terror yesterday even as Sen. Chuck Schumer (D-NY) called the Madrid train bombings a security wakeup call. "I feel perfectly safe," Bloomberg said as commuters prepared for the Monday morning rush hour amid heightened security. "I take the subway virtually everyday. . . . The chances of a terrorist doing damage to you is a lot less than you getting hit by lightning." But Schumer said that while the city and nation have tightened air travel security, subway and rail stations remain vulnerable — and should be equipped with bomb detectors. Source: <http://www.miami.com/mld/miamiherald/business/national/8191148.htm>

8. *March 15, The Trucker* — **ATA's Graves cautions Energy Secretary about diesel prices. The head of the American Trucking Associations (ATA) has asked U.S. Energy Secretary Spencer Abraham to keep an eye on "escalating diesel fuel prices nationwide and the devastating effect they can have on the trucking industry."** In a letter dated March 9, ATA President and CEO Bill Graves urged Abraham to closely track diesel prices, which he said now are averaging more than \$1.60 a gallon, the highest they've been since this time last year. **Graves further stated that diesel is the second highest operating expense after labor for carriers, and that the "surging energy costs could easily act as a roadblock" to the economic recovery path the trucking industry is now on.** Graves asked that the Department of Energy "be sensitive in implementing its policy to boost the reserve's inventory," maintaining that the oil reserve program is adding at least \$4.25 per barrel to the price of crude. Source: http://www.thetrucker.com/stories/03_04/0315_energy_letter.html

9. *March 15, CNN* — **America's risky rails. The tragedy in Madrid may have put an end to the railroad anachronism, the idea that train travel is safer than other modes. The attack that killed some 200 innocents was cruelly simple. The perpetrators left backpacks full of explosives fitted with simple timers and walked away.** Some 10 million train and subway trips are taken every day in America. Amtrak shuttles 66,000 of those passengers, two-thirds of them through the target-rich northeast corridor. The Washington Metro moves 600,000 people near national monuments. What makes trains useful is what makes them devilishly hard to secure: many doors, high volumes of passengers and thousands of miles of lonely tracks. The Federal Government is spending \$4.5 billion on aviation security this year but only \$65 million on rail security even though five times as many people take trains as planes every day. **Since**

2000, bombs have gone off (or been defused) on railways in India, Russia, France, the Philippines, the Czech Republic, South Africa, Israel and Germany. Intelligence sources reported that al Qaeda operatives had cased the Washington rail corridor and that some had discussed exploding a train near storage tanks for hazardous chemicals.

Source: <http://www.cnn.com/2004/ALLPOLITICS/03/15/railsafety.tm/>

10. *March 15, Straits Times Asia (Singapore)* — **Worried Britain boosts rail security.** As Europe beefs up rail security after last week's deadly Madrid bombings, Britain will deploy anti-terror marshals on trains across the country and throughout London's underground network. **Sniffer dogs targeting explosives will patrol railway stations and the government has ordered hundreds of extra closed-circuit television cameras.** Worried that Britain, and particularly its capital, could be the next terrorist target, the government has reopened its secret underground emergency nerve centre near Parliament in central London — codenamed Cobra. Intelligence sources fear that terrorists are planning an attack on Britain for its support of the U.S.-led war in Iraq. It is understood that armed police and even troops may be ordered in to reinforce patrols. In the meantime, undercover officers will ride on trains. **Security officials face a daunting task monitoring Britain's rail network, with thousands of miles of track serving 2,600 stations. Every day, trains carry more than five million passengers.** At train and subway stations across Europe, armed patrols, bomb detection measures and electronic surveillance have been stepped up.

Source: <http://straitstimes.asia1.com.sg/world/story/0.4386.240261.0.0.html?>

11. *March 15, New Straits Times (Malaysia)* — **Study: Mega ports, trade routes vulnerable to seaborne bombs.** The author of a new report on the vulnerability of the global maritime industry said that the deadly train bombings in Madrid last week proved how far terrorists will go to achieve their targets. "They show that despite an international crackdown on al Qaeda and other terrorist networks, extremists retain the capacity to strike viciously," said Michael Richardson, a visiting senior research fellow at Singapore's Institute of Southeast Asian Studies (ISEAS). **The reports says that al Qaeda "aims to disrupt the seaborne trading system, the backbone of the modern global economy, and would use a crude nuclear explosive device or a radiological bomb to do so if it could get its hands on either and position it to go off in a port city, shipping strait or waterway that plays a key role in international trade."** The report also pointed out that while about 80 per cent of international trade by volume is carried by sea, the maritime industry is "poorly regulated, frequently beyond the reach of the law and often secretive in its operations, especially in concealing the real owners of ships." Most seaborne international trade is carried by at least 46,000 ships calling at more than 2,800 ports. There are more than 1.2 million seafarers and hundreds of thousands of port workers, the report said.

Source: http://www.nst.com.my/Current_News/NST/Monday/World/20040315074145/Article/indexb.html

12. *March 15, Department of Transportation* — **DOT seeks applications for nearly \$20 million in grants to improve air service to small communities.** This is the third year the Department of Transportation (DOT) will award grants under the Small Community Air Service Development Program. **Approximately \$19.9 million is available for grants to help communities address their local air service problems, such as high fares and insufficient levels of service.** "The Small Community Air Service Development Program challenges

communities to find new and innovative ways to attract and improve commercial air service," said U.S. Transportation Secretary Norman Y. Mineta. DOT will give priority to those communities that have high airfares compared to other communities, contribute financially to the project from sources other than airport revenues, have established or will establish a public/private partnership to improve their air service, submitted proposals that will benefit a broad segment of the public with limited access to the national transportation system, and will use the assistance in a timely fashion.

Source: <http://www.dot.gov/affairs/dot03004.htm>

13. *March 14, Oakland Tribune* — **Bay Area trains are beefing up security. Security officials have stepped up safety measures at Amtrak rail systems in California and BART in the Bay Area after the bombings in Madrid, last week.** "We're totally vulnerable. I don't know why it hasn't happened yet," said Amtrak conductor Larry Lindbloom, who works the daily route between San Diego and Los Angeles. **Amtrak spokesperson Sarah Swain, based in Oakland, said the rail system has increased security, boosting use of bomb-sniffing dogs as well as patrols by Amtrak officers in conjunction with freight operators and local authorities.** Another Amtrak representative, Dan Stessel, said electronic surveillance of bridges and tunnels was intensified and the company has again urged employees to report suspicious activities to police.

Source: http://cnni.wyellowbrix.com/pages/cnniw/Story.nsp?story_id=48439087&ID=cnniw&scategory=Transportation:Rail&

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

14. *March 15, AgProfessional.com* — **Bird flu testing to expand to cover most U.S. poultry.**

Government and poultry industry officials intend to expand testing for bird flu to cover most of the poultry raised in the U.S., possibly this month, according to an Agriculture Department official. **The \$12.5 million program would focus on the most dangerous forms of the most common variety, low pathogenic avian influenza. These forms, known as H5 and H7, can be no worse than the chicken equivalent of the common cold. If left to spread, however, they can mutate into highly pathogenic varieties that can kill entire flocks in a day.** The new testing system could take effect March 29, assuming it gets final Bush administration approval, said Andrew Rhorer, senior coordinator of the Agriculture Department's Poultry Improvement Plan. The plan was approved on March 5 by a committee of federal, state and industry officials that oversees the program, he said.

Source: http://www.agprofessional.com/show_story.php?id=24076

15. *March 15, AgProfessional.com* — **Canada to ease certain requirements for feeder cattle.**

Canadian officials plan to lift certain requirements for feeder cattle from the U.S., a move they

say will improve year-round access for cattle headed to Canadian feedlots. **Under the rules, testing and treatment requirements for anaplasmosis and the viral disease bluetongue will no longer apply to feeder cattle imported from the U.S., the Canadian Food Inspection Agency said.** Anaplasmosis is caused by a blood parasite and can cause anemia or even death. Insects can spread both diseases. The rules, to take effect April 1, are a "positive recognition of the integrated nature of the industry," said Chris Thomson, consul general for Canada for the Upper Midwest and Rocky Mountain States. Steve Pilcher, executive vice president of the Montana Stockgrowers Association, said his group has been "very adamant and persistent in saying there is no scientific justification for the seasonal restrictions" that have been in place. Currently, feeder cattle from about nine states, including Montana, can enter Canada without testing during the cooler-season months of October through March.

Source: http://www.agprofessional.com/show_story.php?id=24075

16. *March 13, Xinhua News Agency – CEIS* — **Thai government orders new poultry cull as bird flu strikes again. The local government of Uttaradit province of Thailand ordered new slaughter of poultry in three villages of the province with confirmed new outbreaks of bird flu, the Bangkokbiznews.com website reported Saturday, March 13.** The report said after some chickens fed in three villages of the province, 500 kilometers northeast of Bangkok, died recently, the provincial livestock officers took 23 samples of the birds to determine the cause of the death in Phitsanuklok province. The lab test detected the fatal bird flu virus from the sample, then the local government had ordered to cull all of the birds within a one-kilometer radius of where the virus was found. An estimated total of 2,900 poultry will be slaughtered. The Thai government admitted the Kingdom was affected by bird flu on January 23, then declared 43 of the 76 provinces in the nation as bird flu control zones or red zones successively. After more than 35 million poultry was slaughtered, the spread of the fatal virus has been controlled. In February, all of the red zones had been degraded as yellow zones. Thailand's poultry industry, the world's fourth largest, has also suffered much from the bird flu outbreak. The European Union, Japan and other major markets have banned Thai chicken products.

Source: http://cnniw.yellowbrix.com/pages/cnniw/Story.nsp?story_id=48433122&ID=cnniw&scategory=Chemicals:Agricultural&

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

Food Sector

17. *March 15, High Plains Journal* — **Homeland security and local grain elevators. Local elevator managers need to "think like a criminal" in order to identify which parts of their operations could be vulnerable to terrorist or other security threats, according to a production quality expert,** speaking at the annual convention of the National Grain and Feed Association Sunday, March 14. There are "hundreds of ways to contaminate our food supply," warned Paul Stevenson, director of production quality and identity preservation (IP) systems for AIB International in Kansas City, MO. However, he added, there are also steps that can be taken at grain handling facilities to guard against contamination. Stevenson said the first step is for the company to conduct a vulnerability assessment to identify weaknesses. Beyond the vulnerability assessment, each company needs a crisis management plan spelling out steps that would be taken in case of a national emergency, an industry emergency, a facility emergency or

a product recall.

Source: <http://www.hpj.com/dtnnewstable.cfm?type=story&sid=11287>

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

Water Sector

18. *March 15, Associated Press* — **Drought lingers in parts of Colorado. For the first time in several years southwestern Colorado has gotten substantial snowfall, but like the rest of the state the drought won't go away. Reservoir totals are considerably up from last year's record drought, as much as 65 percent in one area, but remain mostly below average.** Butch Knowlton, La Plata County's director of emergency preparedness, keeps a wary eye on daily temperature fluctuations and the Missionary Ridge Fire burn area. The 2002 fire burned more than 70,000 acres, leaving the ground without its usual moisture-absorbing cover. "If we get warm night temperatures with warm daytime temperatures, then you better get your boat (ready)," Knowlton said. A rapid snowmelt could create floods and mudslides. County officials take that possibility seriously enough that this week about 60 regional emergency managers will take part in an exercise at the La Plata County Emergency Coordination Center. "We're going to simulate reservoirs being full and a rainstorm on the remaining snowpack and the problems (that scenario would) create for us," Knowlton said.

Source: http://news4colorado.com/localnews/local_story_075122953.htm

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

Public Health Sector

19. *March 14, Ascribe Newswire* — **Duke University physicians predict risks of deadly infections after cord blood transplants. Transplant physicians at the Duke Comprehensive Cancer Center have identified several risk factors that make certain children more likely than others to die of viral infections after receiving umbilical cord blood transplants to cure their deadly cancers, immune diseases and rare metabolic disorders.** The Duke team has already applied their findings in the laboratory toward strengthening cord blood's ability to wage an immune response. Doctors ultimately plan to infuse these bolstered immune cells into transplant patients to more effectively fend off opportunistic infections, said Paul Szabolcs, M.D., assistant professor of pediatrics and immunology at the Duke Pediatric Bone Marrow and Stem Cell Transplant Program. Children are at highest risk of infection during the first 100 days after transplant, when their new immune system struggles to take hold or "engraft." Even after engraftment occurs, cord blood lymphocytes may remain relatively immature and "naive" to viral infections because they have never been exposed to nor vaccinated against viruses. Szabolcs will present findings of his study at the International Bone Marrow Transplantation Research meeting February 12 – 17, 2004, in Orlando.

Source: http://cnniw.yellowbrix.com/pages/cnniw/Story.nsp?story_id=48453420&ID=cnniw&scategory=Healthcare:Disease&

20. *March 14, Consumers* — **Problems with flu vaccine supply.** This year's flu season brought consumers a double dose of trouble. **First, as is well-known to most, there was not enough**

vaccine made to be given to all who wanted it at the start of this year's apparently harsh flu season. By December 5, many health care providers were starting to turn shot seekers away, and the manufacturers said that all the vaccine they had made had already been shipped. **Second, the vaccine made for the 2003–2004 flu season was not as close a match to the predominant flu virus currently circulating as the government's scientific advisors had wanted it to be—meaning that the vaccine might offer less protection for this season than in seasons past.** A closer examination of what was actually said by the government's vaccine advisors paints a slightly different picture, however. In February and March of 2003, the Vaccine and Related Biological Products Advisory Committee met, as it does every year, to discuss what flu vaccine formulation to recommend to the Food and Drug Administration. Unlike vaccination for other diseases, vaccination against the flu is an annual affair because flu viruses mutate frequently, making any immunity short-lived. The Food and Drug Administration approves a specific flu vaccine formulation for each flu season.

Source: http://cnni.w.yellowbrix.com/pages/cnniw/Story.nsp?story_id=48425028&ID=cnniw&scategory=Healthcare:Immunology&

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

Government Sector

Nothing to report.

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

Emergency Services Sector

21. *March 15, Ithaca Journal* — **NYC holds massive terror drill.** Scenario: A bomb went off in the seats of Shea Stadium. Police detectives hunted for suspects in the pretend chaos. Firefighters hauled out mock victims on stretchers. More than 60 hospitals filled with those playing the injured. **New York's largest terrorism drill since September 11, 2001, unfolded over four chilly hours Sunday, March 14, drawing more than 1,000 police, firefighters and paramedics and an equal number of fire, police and medical trainees playing victims.** Mayor Michael Bloomberg said last week's bombing of commuter trains in Madrid underscored the need for the exercise, the city's 40th designed to help city agencies improve communication and coordination in the face of a potential attack.

Source: <http://www.theithacajournal.com/news/stories/20040315/localnews/81507.html>

22. *March 15, Government Technology* — **New site selected for Illinois state emergency operations center.** Gov. Rod R. Blagojevich has announced the site for the new state-of-the-art State Emergency Operations Center (SEOC). **The proposed site, pending final approval by the federal government, is located on Springfield's east side. "The site is ideal because of its close proximity to a major highway and because it's quickly and easily accessible to all state agency representatives that will be reporting to the center in the event of an emergency,"** said Blagojevich. The center is set to be operational by fall 2005. "The new State Emergency Operations Center (SEOC) will be a big step forward in Illinois' ability to respond to any sort of disaster," Illinois Emergency Management Agency Director William Burke said. "Not only will we have state-of-the-art communications and

information technology in the new SEOC, but we will be bringing our telecommunications center, response center, terrorism intelligence center and radiological assessment center together under one roof." Also slated for the site is the construction of a helipad allowing officials to be quickly transported to a disaster scene nearly anywhere in the state.

Source: <http://www.govtech.net/news/news.php?id=89658>

23. *March 15, Associated Press* — **EU calls emergency meetings on terrorism. The European Union (EU) will hold high-level security talks on Friday, March 19, to assess what additional anti-terrorism measures to take in the wake of the bombings in Madrid, the Irish prime minister announced Monday, March 15.** Prime Minister Bertie Ahern said proposals would include a "solidarity clause" committing nations to help each other in response to terror attacks, the appointment of a special EU official to coordinate counterterrorism operations in Europe, improved intelligence sharing and closer cooperation with non-EU nations to combat terrorism at a global level. "The callous and cowardly attacks on March 11 served as a terrible reminder of the threat posed by terrorism to our society," Ahern said in a statement. "The attacks in Madrid were an attack against the very values on which the Union is founded." The EU foreign ministers will continue the debate the following Monday, before the packages goes to an EU summit, scheduled for March 25-26. All the meetings will be at EU headquarters in Brussels.

Source: http://story.news.yahoo.com/news?tmpl=story&cid=518&e=1&u=/ap/20040315/ap_on_re_eu/eu_terrorism

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

Information and Telecommunications Sector

24. *March 15, TechWeb News* — **New Bagle worm variants sneak past defenses.** Two new versions of the Bagle worm, Bagle.n and Bagle.o, were spotted over the weekend. Unlike earlier editions of Bagle, which tried to circumvent anti-virus software by placing the worm payload into an encrypted .zip archive, **the new Bagles may also use a different archive format, .rar, a file type that consumers are unfamiliar with and enterprises may not block at the gateway.** Additionally, Bagle.n and Bagle.o include the password to the .rar and .zip files in the message not as text, but as an embedded graphic, a tactic often used to discourage automated e-mail account creation by spammers or by Websites to prevent spam bots from harvesting e-mail addresses. When Bagle first turned to encrypted .zip files to disguise its payloads, anti-virus firms reacted by scanning the message for the in-text password. **Shifting to an image of the password may make it tougher for anti-virus programs to unlock the .rar file.** The new Bagles randomly attach their code to 32-bit executables on the infected machine's hard drive and then re-infect a supposedly cleaned system once the executable runs.

Source: <http://informationweek.securitypipeline.com/news/18400151>

25. *March 14, eWEEK* — **Leaked code still could bear malicious fruit.** A portion of Windows source code was leaked last month, and researchers are saying that hackers have uncovered several previously unknown vulnerabilities in the code. Immediately following the code's posting on the Internet, members of the security underground began poring over the code, searching for undocumented features and flaws that might give them a new way to break into Windows machines. The real danger isn't the vulnerabilities that this crowd finds and then

posts; it's the ones that they keep to themselves for personal use that have researchers worried. Experts said there has been a lot of talk about such finds on hacker bulletin boards and Internet Relay Chat channels of late, indicating that some hackers are busily adding new weapons to their armories. Another concern for Microsoft and its customers is that **even though the leaked code is more than 10 years old, it forms the base of the company's current operating system offerings, Windows XP and Windows Server 2003. This means that any vulnerabilities found in Windows NT or Windows 2000 could exist in the newer versions as well.**

Source: <http://www.eweek.com/article2/0.1759.1548988.00.asp>

Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: WORM_NETSKY.C Source: http://wtc.trendmicro.com/wtc/wmap.html , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 80 (www), 445 (microsoft-ds), 3127 (mydoom), 1434 (ms-sql-m), 137 (netbios-ns), 6129 (dameware), 1433 (ms-sql-s), 3410 (---), 1080 (socks) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

26. *March 12, The Independent (Gambia)* — **Over 15,000 gallons of gasoline allegedly missing. The Gambian police are currently investigating the alleged theft of over 15,800 gallons of gasoline, which disappeared from Shell Marketing's fuel depot in Banjul, Gambia on Wednesday, March 10.** Security guards from the Wackenhut Corporation who were posted at the depot are being held over the missing gasoline with several of them charged. Officials at the depot would only confirm the gasoline scam and said that they cannot comment on the matter for fear of prejudicing the outcome of the probe. They said the case is currently under police investigation. The police Public Relations Officer ASP Aziz Bojang said that they have received complaint of a theft case from Shell Marketing, but the police cannot confirm the quantity of gasoline involved.

Source: <http://allafrica.com/stories/200403120445.html>

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

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Warnings](#) – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Publications](#) – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644

Subscription and Distribution Information Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644 for more information.

Contact DHS/IAIP

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 info@us-cert.gov or visit their Web page at www.uscert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.