



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 25 July 2003

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports many Nebraska bank customers lost access to their debit card accounts after a Malaysian counterfeit ring hacked the bank's computer system and attacked its Visa Check Card program to steal debit card numbers. (See item [6](#))
- IDG News Service reports that on July 21, some customers of Wells Fargo bank found themselves the target of an e-mail fraud attempt. (See item [7](#))
- Newsday.com reports that Sunday, on a Rome-to-New York flight, the device that prevents the windshield from fogging up on a Boeing 777 apparently overheated shattering the inside layer and sparking a fire. (See item [9](#))
- The Department of Homeland Security and Microsoft have issued an advisory warning of "Potential For Significant Impact On Internet Operations Due To Vulnerability In Microsoft Operating Systems." (See item [23](#))
- Government Computer News reports the growing integration of digital control systems with traditional computer networks is opening a new avenue of attack against the nation's physical infrastructure. (See item [24](#))

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. *July 24, The Tennessean* — **TVA plant fire forces closure of damaged turbines. A fire broke out Wednesday, July 23, at 4:40pm at the Tennessee Valley Authority's coal-fired New Johnsonville power plant located in New Johnsonville, TN.** At one point during the blaze, the fire affected three of the ten 150-MW turbine units. The plant was shut down as a precautionary measure. **A TVA spokesman said the cause of the fire was not immediately known. The damaged turbines probably will be off-line for several weeks, but TVA said that this would not create a power shortage.**
Source: http://www.tennessean.com/local/archives/03/07/36484494.shtml?Element_ID=36484494
2. *July 24, Reuters* — **Constellation shuts Nine Mile nuke. Constellation Energy Group Inc. shut its 1,105 megawatt Nine Mile Point 2 nuclear unit in upstate New York on Thursday, July 24, for repairs.** Industry sources familiar with the plant's operation said it was shut to correct a relay power supply problem, however, Constellation officials said they would provide further details on the outage later in the day.
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2003_07_24_eng-reuters_pma_CONSTELLATION-SHUTS-N-Y-MW-NINE-MILE-NUKE&SMContentSet=0
3. *July 23, abc7.com* — **Refinery explosion in California. A steam boiler exploded Wednesday, July 23, at a refinery in Carson, CA, a suburb of Los Angeles.** No injuries occurred, but officials did shut down operations at the plant as a precautionary measure. The explosion at the refinery, owned by Conoco Phillips, happened around 6:25am. "It was a significant explosion," producing "a lot of debris," said Capt. Mark Savage of the Los Angeles County Fire Department, but **"there was no leak of any petroleum product."** Experts worked to determine the cause of the blast in the steam boiler. A damage estimate was not immediately available.
Source: http://abclocal.go.com/kabc/news/072303_nw_refinery_fire.html

[[Return to top](#)]

Chemical Sector

4. *July 24, Associated Press* — **Dow Chemical posts \$393 million profit. Dow Chemical Co.'s second quarter profit rose 65 percent, beating Wall Street expectations, as higher sales and cost-cutting offset higher feedstock and energy costs, the company said Thursday.** For the three months ended June 30, Midland-based Dow earned \$393 million, or 43 cents a share, compared with \$238 million, or 26 cents a share in the same period last year. "In spite of the huge challenges faced by industry in the second quarter ... Dow has responded well," said J. Pedro Reinhard, executive vice president and chief financial officer. "This is primarily due to the company's focus on the financial discipline implemented since the beginning of the year. In January, the company announced plans to cut between 3,000 and 4,000 jobs, many through attrition or as part of trades or sales of holdings. The company had 50,000 employees at the end of 2002. **The chemical company said feedstock and energy costs increased by about \$700**

million compared to a year ago, but agricultural sciences posted record sales results for the quarter and joint ventures earnings were up.

Source: <http://www.timesdaily.com/apps/pbcs.dll/article?AID=/20030724/APF/307240727>

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

Defense Industrial Base Sector

5. *July 24, The New York Times* — **GAO faults cost estimates on Boeing–Air Force jet lease. In testimony before the House Armed Services Committee on Wednesday July 23, the General Accounting Office (GAO) estimated that the price of each Boeing 767 the Air Force planned to lease from Boeing would be \$173 million, not the \$138 million put forth by the Air Force and Boeing.** Neil Curtain, the GAO's manager for defense capabilities, said his agency's price estimate assumed the Air Force would buy each aircraft at the end of the six–year lease. The Air Force–Boeing estimate of \$138 million per plane did not include a final purchase price at the end of the lease. The Boeing 767's would be used as aerial refueling tankers, and the Air Force would like to lease 100 of them, which makes the plan controversial because the planes would be leased, rather than bought outright, as is the case with most military equipment. The GAO testimony is available at <http://www.gao.gov/new.items/d031048t.pdf>
Source: <http://www.nytimes.com/2003/07/24/business/24JETS.html>

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

Banking and Finance Sector

6. *July 23, Associated Press* — **Counterfeit ring hacks Nebraska bank's computer. Some customers of the Platte Valley Bank in Kearney, NE, lost access to their debit card accounts after a Malaysian counterfeit ring hacked the bank's computer system and attacked its Visa Check Card program to steal debit card numbers. The bank became aware of the illicit activities when their high–tech trip wires discovered the unauthorized transactions.** According to the bank, only a small number of customers were affected, and they will be issued a new debit card with a new account number. Bank president Mark Sutko said that law enforcement officials would not be contacted about the situation and the bank is handling the problem internally.
Source: http://www.usatoday.com/tech/news/computersecurity/2003-07-23-ne-hack_x.htm
7. *July 23, IDG News Service* — **Wells Fargo customers hit with e–mail scam.** On Monday, July 21, some customers of Wells Fargo bank found themselves the target of an e–mail fraud attempt. Customers received an e–mail from "Wells Fargo Accounting" regarding a new account application that contained an attachment, that, if opened, would download software onto the customer's computer, gather passwords, and send them to an unauthorized third party, presumably to the originator of the e–mail, the bank said. Wells Fargo stated that the e–mail was a hoax, and urged recipients to delete both the e–mail and the attachment. It wasn't immediately clear how many customers had been affected by the scam, and Wells Fargo said its systems had not been compromised in any way.

Source: http://www.idg.net/ic_1327167_9677_1-5046.html

8. *July 23, finextra.com* — **Computer glitch knocks out Mizuho settlement system. Japan's Mizuho Corporate Bank failed to settle five thousand overseas deals on Tuesday, July 22, after experiencing a glitch in its computerized settlement system.** The bank experienced a systems problem that affected custody transactions with about 30 firms. Although the problem was fixed on Tuesday, about 1800 transactions remained unsettled by late Wednesday, July 23, because of a processing delay, the bank said.

Source: <http://www.finextra.com/fullstory.asp?id=9539>

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

Transportation Sector

9. *July 24, Newsday.com* — **Plane's windshield shatters.** On a Rome-to-New York flight, this past Sunday, an Alitalia jet had what the crew termed a "major" technical problem, made a U-turn over the ocean, and headed back to land, where emergency rescue crews were waiting at the airport in Shannon, Ireland, an hour later. **After landing, it was obvious that the windshield above the captain's seat in the Boeing 777 was shattered, with blankets and pillows from the cabin piled up behind it. Boeing officials say the device that prevents the windshield from fogging up apparently overheated, shattering the inside layer and sparking a fire.** The pilots put out the fire in the cockpit with a fire extinguisher, but the inner layer of the acrylic-glass material that makes up the windshield began to splinter, with pieces falling into the cockpit. If an aircraft at a high altitude – the Alitalia plane was at 39,000 feet – loses pressurization, the flight crew is at risk of being sucked out. The Alitalia jet quickly descended to close to 10,000 feet, where pressurization is not an issue. **It's not the first time the windshield on a Boeing 777 has shattered when the heating element malfunctioned.** Federal Aviation Administration records show two instances of windshields on the world's largest twinjet shattering in the past year.

Source: <http://www.newsday.com/news/local/longisland/ny-liwind243385759jul24.0.1538434.story?coll=ny-linews-headlines>

10. *July 24, Reuters* — **JetBlue posts profit like other low-cost carriers. JetBlue Airways Corp. Thursday posted a second-quarter profit of \$38 million including reimbursement for security fees, the latest low-cost carrier to outperform its bigger rivals amid a weak U.S. travel market. JetBlue, a 3-year-old airline based in New York, has won over passengers from bigger rivals with its low fares, leather seats and live television.** During the second quarter, the government reimbursed U.S. airlines for security fees as the Iraq war cut into travel demand nationwide. JetBlue received \$23 million. Other low-cost airlines posting income, even without the government handouts, were Southwest Airlines Inc. and America West Holdings Corp. and Alaska Air Group Inc. Posting operating losses in the second quarter were American Airlines parent AMR Corp. , Delta Air Lines Inc. , Continental Airlines Inc. and Northwest Airlines Inc.. **Revenue for U.S. carriers fell sharply in the quarter, generally, as the Iraq war kept passengers out of the skies and the deadly SARS virus spread through Asian countries.**

Source: <http://www.forbes.com/markets/newswire/2003/07/24/rtr1036330.html>

11. *July 24, Associated Press* — **Union Pacific beats Wall Street estimates.** Union Pacific Corp., battling high diesel fuel prices and a slow economy, said Thursday that second quarter profits fell 5 percent to \$288 million, still enough to beat Wall Street estimates. **The company that owns the nation's largest railroad said net income came to \$1.10 per share, compared to \$304 million, or \$1.15 per share in the second quarter of 2002. Union Pacific's steady business hauling farm products and coal helped make up for a weak quarter for carrying consumer goods like television sets and cars,** the company said. "In a weak economic climate with car loadings flat compared to last year, this excellent revenue performance indicates the strength of our business mix," chairman and chief executive Dick Davidson said. Union Pacific's trucking company, Overnite Corp., had a 15 percent increase in its second quarter operating income to \$21 million from \$18.2 million in the same period last year. **Diesel fuel and natural gas prices remain high, creating a drag on the economy and affecting Union Pacific and its customers,** Davidson said.

Source: <http://www.nytimes.com/aponline/business/AP-Earns-Union-Pacific.html>

12. *July 23, Associated Press* — **House GOP would give Amtrak \$900M in aid. House Republicans prepared a revamped transportation bill on Wednesday that would give Amtrak \$900 million next year, more than an earlier version but half what the financially struggling passenger railroad says it needs to maintain existing service.** The House Appropriations Committee planned to approve the legislation on Thursday, nearly two weeks after that panel's transportation subcommittee signed off on an initial measure providing only \$580 million for Amtrak. The new version has \$900 million for Amtrak, said a GOP aide speaking on condition of anonymity. That would be the same amount as President Bush requested. But an Amtrak spokesman, Clifford Black, said that "would be a nonstarter" because the railroad needs improvements for its tracks, cars, tunnels and other equipment. **The rewritten bill also eliminates cuts that would have been made in mass transit construction, bicycle trails, subsidies to air carriers that serve rural communities, and other projects, said aides and lawmakers familiar with the bill.**

Source: <http://www.nytimes.com/aponline/national/AP-Congress-Spending.html>

[[Return to top](#)]

Postal and Shipping Sector

13. *July 24, DM News* — **Postal Panel puts forth new recommendations. Personalized postage stamps, a security system to track mail, and fewer postal employees were among the recommendations yesterday from two subcommittees of the President's Commission on the U.S. Postal Service.** "The postal service will soon be presented with a unique attrition opportunity with 47 percent of current career employees eligible for retirement by 2010," it said. **"The workforce subcommittee urges the postal service to take full advantage of this attrition opportunity and to exercise maximum discipline in its hiring practices in order to right-size and realign its workforce with minimal displacement."** The technology challenges subcommittee recommended that the postal service automate more systems and outsource what it can to other companies. It also suggested studying mail processing with the goal of redesigning the entire system with the latest technology. Other recommendations included: **putting mail tracking technology in place on a timely and more comprehensive basis, integrating its facility automation efforts with its transportation network by using**

Intelligent Mail technology, GPS, and onboard computer technology, and in coordination with the Department of Homeland Security, explore the use of sender identification for every piece of mail, commercial and retail.

Source: http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=24583

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

Agriculture Sector

14. *July 24, CanWest News Service* — **Expert predicts long ban on cattle. Borders won't reopen to live cattle from Canada for years, says a top official with the Canadian Food Inspection Agency, a ban that could erase a \$1.8 billion industry.** Francine Lord, national manager of imports and exports for the agency, said countries would likely consider Canadian cattle too risky, but expects trade would resume in beef, bovine semen, and embryos if borders opened again to ruminants, or cud-chewing animals. More than 30 countries banned Canadian cattle and beef after the country discovered its first homegrown case of mad cow disease on May 20. "We don't have any tests for live animals. That's the problem," Lord said. "If we have tests on live animals, it would be easy." **Lord expects exports of feed made from ruminants won't resume either. Cindy McCreath, spokeswoman for the Canadian Cattlemen's Association, said cutting off trade for years to live cattle would cause great problems for the industry, but it could recover as long as borders reopened to beef.**

Source: <http://canada.com/national/story.asp?id=7E1FAC17-91E3-4465-BCF0-923DF591934C>

15. *July 23, Farming Life* — **South America on way to cattle IDs.** Brazil and Uruguay have announced they are one step closer to individual cattle identification. **Argentina announced that, from July 1, 2003, all cattle entering export abattoirs must be tagged.** Producers have until August 15, 2003 to ensure all cattle destined for export establishments are tagged at least 40 days prior to slaughter. **Brazil also now has a cattle identification system in place,** whereby all cattle destined for export processing plants must be tagged at least 40 days before slaughter. **Uruguay continues to have a voluntary cattle identification system.** However, one million tags are being purchased, which is seen as a step closer to total cattle identification. Traceability is becoming one of the most prominent discussion points between global trading partners. The European Union introduced mandatory traceability following BSE in 2001 and requires it of its suppliers.

Source: http://www.farminglife.com/fl2/content_objectid=13206679_metadata=full_siteid=51658_headline=-South-America-on-Way-to-Cattle-IDs-name_page.html

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

Food Sector

16. *July 24, Crop Decisions* — **USDA reviews changes made by meat packers. The U.S. Department of Agriculture (USDA) is now reviewing safety changes made by beef packers nationwide in response to the massive beef recall last year by the ConAgra Beef Company.** USDA Food Safety Undersecretary Elsa Murano says the USDA asked packers last year to

"reassess" their Hazard Analysis and Critical Control Point (HACCP) systems to better protect against contamination with the E. coli bacteria. Murano says that packers have completed revamping their HACCP systems, and the USDA's Food Safety Inspection Service is now auditing those changes. The results of the FSIS audits will not be made public.

Source: http://www.cropdecisions.com/show_story.php?id=20527

17. *July 24, Pittsburgh Post Gazette* — **FDA announces research effort to protect imported food supply. The U.S. government Wednesday launched a new research project to plug gaps in the security shield being built to guard the U.S. food supply from terrorist attacks.** It focuses on the growing amount of fresh fruits and vegetables now being imported from foreign countries. **About 40 percent of fresh fruit and 15 percent of vegetables eaten in the U.S. are imported.** "A terrorist attack on the food supply could pose both severe public health and economic impacts, while damaging the public's confidence in the food we eat," said Mark B. McClellan, chief of the Food and Drug Administration (FDA). **The program is believed to involve research into technologies such as electronic sensors that could rapidly screen incoming food shipments for contamination by chemical and biological agents and radioactive materials.** FDA said the research marks the start of a new phase in food monitoring programs because the technology would be dual purpose, detecting both terrorists tampering and natural contaminants such as microbes that cause food poisoning. The agency also has been seeking technology that would replace the spot-check system, in which inspectors actually test only a few samples from huge shipment of food.

Source: <http://www.post-gazette.com/pg/03205/205040.stm>

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

Water Sector

Nothing to report.

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

Public Health Sector

18. *July 24, Reuters* — **Hong Kong tests 12 for SARS. Twelve people in Hong Kong, most of them from a mental institution, have been admitted to hospital as suspected Severe Acute Respiratory Syndrome (SARS) cases, raising fears of a resurgence of the disease. A government official said on Thursday the 12 were being tested and it was unclear when the results would be released.** "All of them have respiratory problems such as fever and coughs. They're now under observation and are in stable condition," the government spokeswoman said. She had no further details. Hong Kong is just starting to recover from the devastating effects of a SARS epidemic earlier this year, which killed about 300 people and ravaged the economy. If the tests are positive, it would be a major blow to the city and the government, which has faced massive protests over its handling of the earlier SARS outbreak and a deeply unpopular security bill. **The suspected cases come about one month after the World Health Organization declared Hong Kong free of SARS.**

Source: http://reuters.com/newsArticle.jhtml?type=topNews&storyID=31_52809

19. *July 24, Optics.org* — **Waveguide senses bacteria fast. Scientists in Denmark have built an optical waveguide sensor that detects bacteria using evanescent waves. The sensor could have a multitude of applications in food safety, medical diagnostics and detection of biological war agents.** Henrik Pedersen and colleagues at Riso National Laboratory used the device to monitor levels of Escherichia coli K12 cells in a solution. **The current standard test for 'rapid' bacteria detection, called enzyme-linked immunosorbent assay (ELISA), takes 18–24 hours to give a result and the Riso team believes that there is a large demand for much faster bacteria detectors.** Their detector makes use of the evanescent field. In Pedersen's experiment, the bacterial solution containing Escherichia coli K12 was flowed past the sensor surface for 45 minutes. After that, the change in refractive index caused by the bacteria could be seen. The Riso team estimates the detection limit of the sensor at 60 cells per mm², which is almost three orders of magnitude better than previous optical detection methods. Source: <http://optics.org/articles/news/9/7/17/1>

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

Government Sector

20. *July 24, Federal Computer Week* — **States avoid tax hikes. In the midst of the worst fiscal crisis in decades, state governments have used rainy day funds, specific fee increases and spending cuts to balance their budgets without relying heavily on broad tax hikes, says a report issued this week by the National Conference of State Legislatures.** The report includes information from 43 states, and indicates that states collectively have had to close a \$200 billion budget gap over the past three years. Six states — Alabama, California, Connecticut, Nevada, Oregon, and Pennsylvania — had not enacted their budgets in time for the report, and Michigan had just finished passing its budget. In a separate conference session, David Wyss, chief economist with Standard & Poor's, said the economy is recovering, but at "half-speed or two-thirds speed" than previous recoveries. "That's all we're going to get," he said. **However, he said the risk of recession remains if there are further terrorist attacks or war in the Middle East is expanded.**

Source: <http://www.fcw.com/geb/articles/2003/0721/web-gaps-07-24-03.asp>

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

Emergency Services Sector

21. *July 24, Federal Computer Week* — **Emergency teams get new tech.** Federal emergency workers in the field will get their own communications systems. **The Department of Health and Human Services is equipping vans of the Secretary's Emergency Response Teams with laptop computers and satellite communications,** said KC Decker, a program analyst in the department's Office of the Assistant Secretary for Public Health Emergency Preparedness. "The footprint they would take to the locale would be very small," Decker said, speaking at the GovSec conference in Washington. "It would basically have all the communications equipment you can carry." **The teams, which would be deployed in case of an emergency or terrorist attack, would be able to use the devices in their vans to communicate with department headquarters without interfering with other communications systems.** Decker said HHS'

Response Technology Team is in the process of equipping these vans, and it is unclear when they will be operational. **The teams are centrally-based groups of experts from agencies such as the National Institutes of Health, Centers for Disease Control and Prevention and Food and Drug Administration.** Each team has about eight to 10 members, Decker said, and can be deployed across the country within 24 to 48 hours of an incident. The concept is part of the Federal Response Plan.

Source: <http://www.few.com/few/articles/2003/0721/web-hhs-07-24-03.a.sp>

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

Information and Telecommunications Sector

22. *July 24, General Accounting Office* — **GAO Report GAO-03-1037T: Further Efforts Needed to Implement Statutory Requirements in DOD.** The Department of Defense (DOD) faces many risks in its use of globally networked computer systems to perform operational missions. **Weaknesses in these systems, if present, could give hackers and other unauthorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive military data.** This report discusses the DOD's efforts to protect its information systems and networks from cyber attack, focusing on its reported progress in implementing statutory information security requirements.

Source: <http://www.gao.gov/highlights/d031037thigh.pdf>

23. *July 24, Department of Homeland Security* — **Potential For Significant Impact On Internet Operations Due To Vulnerability In Microsoft Operating Systems. The recently announced Remote Procedure Call (RPC) vulnerability in computers running Microsoft Windows operating systems could be exploited to allow the execution of arbitrary code or could cause a denial of service state in an unprotected computer.** Because of the significant percentage of Internet-connected computers running Windows operating systems and using high speed connections (DSL or cable for example), **the potential exists for a worm or virus to propagate rapidly across the Internet** carrying payloads that might exploit other known vulnerabilities in switching devices, routers, or servers. Due to the seriousness of the RPC vulnerability, the Department of Homeland Security / Information Analysis and Infrastructure Protection National Cyber Security Division and Microsoft encourage system administrators and computer owners to take this opportunity to update vulnerable versions of Microsoft Windows operating systems as soon as possible. A patch is available on the Microsoft Website: <http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp>.

Source: <http://www.nipc.gov/warnings/advisories/2003/Potential72403.htm>

24. *July 23, Government Computer News* — **NDU prof: digital control systems can weaken security. The growing integration of digital control systems with traditional computer networks is opening a new avenue of attack against the nation's physical infrastructure,** John H. Saunders, a professor at the National Defense University, said Wednesday, July 23, at the GOVSEC security conference in Washington. **Controls for operating utilities, buildings and campuses are being turned over to cost-effective digital systems with remote access capabilities.** Proprietary protocols and single-purpose firmware have offered a degree of security for these systems. But standardizing on a few protocols is increasing the risk. Digital

control systems also are being connected to LANs, WANs and the Internet for remote administration. Government administrators can do little about the level of security at utilities, but they can increase security within their own buildings, Saunders said. **Building engineers need to focus on security the way systems administrators do, by performing systems inventories and vulnerability and risk assessments, and by implementing policy**, he said. Source: http://www.gcn.com/vol1_no1/daily-updates/22860-1.html

25. *July 23, Federal Computer Week* — **Security adviser warns of cyberthreats. Officials must still figure out how to fully secure the nation's critical infrastructure against cyber attacks**, said General John Gordon, retired lieutenant general from the U.S. Air Force, presidential assistant and adviser to the Homeland Security Council Tuesday, July 22. **Attacks over electronic networks might become a threat as great as weapons of mass destruction**, he told a meeting of the National Infrastructure Advisory Council in Washington, DC. The council, which consists of a gathering of industry and government officials, is expected to issue recommendations for tougher information security protections in October. One of the council's toughest challenges is **determining what should be disclosed to private industry and the public and when it should do so**, officials told the council. Source: <http://www.few.com/few/articles/2003/0721/web-secure-07-23-03.asp>

Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 2 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: WORM_KLEZ.H 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	137 (netbios-ns), 445 (microsoft-ds), 80 (www), 1434 (ms-sql-m), 56403 (----), 113 (ident), 139 (netbios-ssn), 4662 (eDonkey2000), 20230 (----), 0 (----) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

26. *July 24, Associated Press* — **Glacier National Park evacuated as Montana wildfire grows. Hundreds of hikers, campers and park employees were told to leave part of Glacier National Park on Thursday, July 24, after a wildfire doubled to at least 6,000 acres. In central Idaho, flames overran and killed two firefighters who had just rappelled to the ground to**

clear a helicopter landing zone Wednesday, July 23. **All firefighters were pulled from the blaze in the Salmon–Challis National Forest** and an investigation of the deaths was under way. It was unclear when the fight to contain the blaze would resume. **Another Idaho blaze grew to about 14,000 acres in the Boise National Forest and was about three miles away from the small town of Atlanta on Wednesday evening.** The National Interagency Fire Center said there were 49 large fires burning in the West, with 359,380 acres of active wildfires. Other states with large fires included Arizona, California, Colorado, Montana, New Mexico, Nevada, Oklahoma, Oregon, South Dakota, Utah, Washington and Wyoming. Source: <http://www.nytimes.com/aponline/national/AP–Wildfires.html?h p>

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

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 703–883–6631

Subscription and Distribution Information Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703–883–6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202–323–3204.

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.