



# National Infrastructure Protection Center NIPC Daily Open Source Report for 10 March 2003

Current Nationwide  
Threat Level is



[For info click here](#)

[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

## Daily Overview

- Secretary of Homeland Security Tom Ridge announced on Thursday that nearly \$600 million has been made available to the states and U.S. territories to better assist state and local public safety and law enforcement personnel in preventing, preparing for and responding to terrorism. (See item [21](#))
- CNET News reports the Internet Software Consortium is reporting a remote buffer overflow bug in BIND 9.2.1 when the software is installed with the "libbind" nondefault option. (See item [22](#))
- SecurityFocus reports a Windows root kit (an assembly of programs that subverts the Windows operating system at the lowest levels) called "ierk8243.sys" was discovered on the network of Ontario University last January. (See item [23](#))

### NIPC 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](#); [NIPC 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 07, Platts Global Energy News* — **IEA ready to act if OPEC fails to meet shortage.** The International Energy Agency's (IEA) executive director Claude Mandil Friday reiterated plans to wait and see how OPEC producers react to any supply crunch before deciding whether to release emergency stocks onto the market. **In talks in Riyadh this week, Mandil said Saudi Arabia's oil minister Ali Naimi had pledged to boost output from the 11-member cartel and particularly the kingdom in the event of U.S.-led war against Iraq.** "What is key from my talks with Ali Naimi is the commitment by the kingdom and other producers to increase

production to meet a (supply) shortage. If that is not enough, then action will be taken by the IEA," Mandil told Platts. Asked if he thought OPEC had enough spare capacity to deal with a possible supply disruption from Iraq, he said "we have identified Saudi Arabia and to a lesser extent the UAE as the main countries with spare capacity." **U.S. energy secretary Spencer Abraham earlier this week said that Washington was ready to act quickly to counter a "severe" disruption to supply, but would first consult the IEA before releasing crude from the national reserves.**

Source: <http://www.platts.com/stories/home2.html>

2. *March 07, Platts Global Energy News* — **Iran uranium technology stuns experts. Iran is believed to have quietly developed an advanced supercritical gas centrifuge for uranium enrichment, using a collection of design data obtained in part from non-Western third parties, Western government officials have told Platts. The Iranian centrifuge appears to be a hybrid design, not quite like any other known.** Supercritical centrifuges can enrich uranium faster than subcritical machines that work at lower speeds. Uranium enriched to low concentrations is used for nuclear power reactor fuel; in high concentrations, it can be used for bombs. In all known centrifuge development programs, supercritical centrifuges were developed only after years of experience enriching uranium using subcritical machines. **The latest information given Platts suggests that Iran's uranium enrichment program may be technically more advanced than most experts thought.**

Source: <http://www.platts.com/stories/home1.html>

3. *March 07, New York Times* — **State consultant reiterates: Indian Point plan is weak. After hearing from a range of individuals, government officials and institutions, a consultant hired by the state has reaffirmed his warning that emergency plans for the Indian Point nuclear power plant cannot protect the public from a large release of radiation.** The consultant, James Lee Witt, a former director of the Federal Emergency Management Agency, plans the release today of his final report, which defends and clarifies some points in his original report but does not change his primary conclusion. "The comments that addressed major, substantive issues were not sufficiently compelling that the draft's major findings, conclusions, and recommendations needed to be changed in the final report," according to an excerpt from the final report provided to The New York Times in response to inquiries. **Witt's report, which predicted that an evacuation could be hampered by panicked residents clogging roads, emergency workers unwilling or unable to respond and other uncertainties and problems, energized a campaign by citizens groups, environmentalists and elected leaders to close the plant, 35 miles north of Midtown Manhattan in the Westchester village of Buchanan, N.Y.** The report motivated members of Congress to hold hearings and other forums on the emergency plan, which includes steps for evacuating people within a federally mandated 10-mile radius of the plant. Congress has ordered the Federal Emergency Management Agency to respond to the report by March 25.

Source: <http://www.nytimes.com/2003/03/07/nyregion/07NUKE.html?ntem=ail1>

[[Return to top](#)]

## **Chemical Sector**

Nothing to report.

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

## **Defense Industrial Base Sector**

Nothing to report.

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

## **Banking and Finance Sector**

4. *March 09, Los Angeles Times* — **Five suspects helped fund al Qaeda, Spain says.** Spanish investigators have dismantled an al Qaeda money–laundering operation allegedly run by four Spaniards and a Pakistani linked to the deadly bombing of a synagogue in Tunisia last year, authorities said Saturday. After raids Friday and early Saturday by the paramilitary Guardia Civil in the Spanish cities of Valencia and Logrono, authorities accused the suspects of using their companies to send funds to Al Qaeda operatives around the world. **The four suspects in Valencia are Spanish entrepreneurs whose firms make ceramics and decorative tiles. Initial reports Friday night had described them as Tunisians. The arrests make this one of the few cases in Europe in which apparently non–Muslim, non–Arab businesspeople allegedly played a financial role in Islamic terrorist activity.** The suspects in Spain allegedly helped fund a network in France, Germany and Pakistan that bombed a synagogue on the Tunisian island of Djerba last April, killing 21 people. Authorities say the suicide attack was ordered by Khalid Shaikh Mohammed, the Al Qaeda operations chief arrested in Pakistan last weekend. **"They apparently had contact with members of this organization, and these contacts are with people who had a lot to do with the attack that took place in Djerba," Spanish Interior Minister Angel Acebes said at a news conference in Madrid.**  
Source: <http://www.latimes.com/news/nationworld/world/la-fg-arrests9-mar09004511.1,5637370.story?coll=la%2Dheadlines%2Dworld>
5. *March 08, New York Times* — **Insurance for terrorism still a rarity.** With government officials warning of renewed terrorist attacks in the United States, most of corporate America still has no insurance coverage for acts of terrorism. Last fall, at the insistence of President Bush, Congress provided federal support for insurance companies, and they began offering the coverage in late November. But few corporations in New York, Washington, Chicago or other big cities – where the authorities say attacks are most likely – have bought the coverage. **Many corporations say the coverage is too expensive, according to insurers, especially since the federal government has agreed to pay most of the losses in a major attack. They also say that while the insurance provides economic protection against bombs and many other kinds of violence from foreign terrorists, it does not cover attacks by American extremists or attacks by anyone with nuclear, chemical or biological weapons. Moreover, insurers and brokers say, most corporations simply refuse to believe that they are potential targets.**  
Source: <http://www.nytimes.com/2003/03/08/business/08INSU.html>
6. *March 07, The Cincinnati Enquirer* — **Pull–tab lottery tied to terror.** State authorities are investigating whether a pull–tab lottery game that was supposed to benefit charities in Ohio instead funneled nearly \$500,000 to Islamic terrorists in the Middle East. **Details about the investigation emerged Thursday in Cincinnati during the sentencing of Philip George, an**

**Akron man who was convicted of skimming money from the sale of instant lottery tickets at Ohio bars. An investigator for the Ohio Department of Public Safety testified that at least some of the money that George raised through the lottery has been linked to the militant terrorist groups Hezbollah and Hamas.** George's attorney, Robert Gutzwiller, described the allegations as "balderdash" and said his client has no connection to terrorists. But the state investigator, Harold Torrens, testified that at least \$234,000 in lottery proceeds was sent to the United Saghbeen Society.

Source: [http://enquirer.com/editions/2003/03/07/loc\\_george07.html](http://enquirer.com/editions/2003/03/07/loc_george07.html)

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

## **Transportation Sector**

- 7. *March 07, Associated Press* — DFW airport OKs terrorism insurance policy.** If the Dallas/Fort Worth International Airport were to be attacked by terrorists, a new insurance policy would pay up to half a billion dollars to repair or rebuild it. FM Global insurance company would **cover from \$5 million to \$500 million in damage, as long as the federal government certified that foreign terrorists were responsible.** Otherwise, the policy would pay up to \$100 million. **The terrorism coverage for the nation's sixth-largest airport, approved Thursday by the DFW airport board, will cost \$156,540 annually.** The policy will be in effect until next March. Los Angeles International Airport is covered for up to \$100 million for certified foreign attacks only. Chicago's O'Hare Airport is covered for \$1 billion against certified and noncertified attacks and pays for that thorough coverage with a \$4 million annual premium.

Source: <http://www.chron.com/cs/CDA/story.hts/business/1808943>

- 8. *March 07, U.S. Department of Transportation* — Matthews named DOT Chief Information Officer. U.S. Transportation Secretary Norman Y. Mineta announced on Friday the appointment of Daniel P. Matthews as the Chief Information Officer (CIO) for the U.S. Department of Transportation (DOT).** As CIO, Matthews will serve as the principal advisor to the Secretary on matters involving information resources and information services management, and provide leadership in using information technology to achieve the department's goals and objectives. "Dan's more than 30 years of experience in information technology will be invaluable to the department as we continue to enhance the efficiency and security of our information systems," Secretary Mineta said. "I welcome him to our team."

Source: <http://www.dot.gov/affairs/dot01903.htm>

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

## **Postal and Shipping Sector**

Nothing to report.

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

## **Agriculture Sector**

9. *March 07, Great Falls Tribune* — **75,000 fish destroyed at hatchery. Fish managers destroyed nearly 75,000 rainbow trout and Arctic grayling at Big Spring Trout Hatchery in Lewistown, MT this week after some fish there tested positive for a pathogen that causes bacterial kidney disease (BKD).** A small percentage of rainbow trout and grayling tested positive in mid-February, during a routine annual health inspection of the hatchery. BKD is a stress-related bacterial pathogen that attacks the kidneys of fish. Based on the positive test, hatchery officials euthanized 30,100 grayling and 44,825 rainbows. The fish were five inches long. **The Lewistown hatchery remains quarantined but tests will continue there. The Lewistown trout hatchery raises 1.8 million fish annually.**

Source: [http://www.greatfallstribune.com/news/stories/20030307/local\\_news/1127423.html](http://www.greatfallstribune.com/news/stories/20030307/local_news/1127423.html)

10. *March 07, Associated Press* — **4.7 million chickens quarantined. Connecticut officials said Thursday they have quarantined 4.7 million chickens as they investigate a possible outbreak of avian influenza at an egg farm, a move that prompted Japan to temporarily ban U.S. poultry imports.** Acting Agriculture Commissioner Bruce Gresczyk said samples from the farm have been sent to a laboratory in Iowa and results are expected next week. Gresczyk said the particular strain suspected is considered a low-grade pathogen and in some cases is not fatal to chickens. But if influenza is confirmed, the state may have to destroy the flock, Gresczyk said. **The egg industry is among the top agriculture businesses in Connecticut, with annual receipts of between \$60 million and \$100 million.**

Source: <http://www.cnn.com/2003/US/Northeast/03/06/chicken.quarantine.ap/index.html>

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

## Food Sector

Nothing to report.

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

## Water Sector

11. *March 07, Hoover's* — **Desalination plan begins in Los Angeles area. Looking to lessen its dependence on imported water, the Calleguas Municipal Water District, in California, will launch an ambitious plan this month to remove salt from the groundwater under the Simi and Conejo valleys and make it drinkable.** Calleguas officials envision a series of desalination plants able to convert up to 30,000 acre-feet a year of brackish groundwater into potable supplies, a yield equal to one-fourth of what the region imports annually. They plan to break ground this month on a \$65 million, 32-mile pipeline, stretching from Simi Valley to Oxnard, that will carry the concentrated saltwater from desalination plants in Simi Valley, Camarillo and the Las Posas Valley to the Pacific Ocean. **Ventura County isn't the only region seeking to reclaim tainted water. From Los Angeles to San Diego there are some 16 million acre-feet of groundwater that cannot be tapped because of high salt content or contamination, according to the Metropolitan Water District.**

Source: [http://hoovnews.hoovers.com/fp.asp?layout=query\\_displaynews&q=WATERsd=ERR200303071180.3\\_359d001e48fe9c34](http://hoovnews.hoovers.com/fp.asp?layout=query_displaynews&q=WATERsd=ERR200303071180.3_359d001e48fe9c34)

12. *March 07, Water Tech Online* — **U.S. water ranked 12th in worldwide water quality report. The United States ranks 12th in the world in water quality among 122 nations, according to a report issued by the United Nations Educational Scientific and Cultural Organization (UNESCO).** The report took an in-depth look at every major dimension of water use and management, from the growth of cities to the threat of looming water wars between countries, the UN report said. The report ranked 122 countries according to the quality of their water as well as their ability and commitment to improve the situation, UN officials said. **The rankings were composite figures based upon a range of factors such as the quantity and quality of freshwater, especially groundwater, wastewater treatment facilities as well as legal issues such as the application of pollution regulations, UNESCO said.**  
Source: <http://www.watertechonline.com/news.asp?mode=4font>>

[[Return to top](#)]

## **Public Health Sector**

13. *March 07, Associated Press* — **Two women, not vaccinated for smallpox, develop eye infections from vaccine. Two women developed infections after touching soldiers who had been vaccinated against smallpox and then touching their eyes.** Both illnesses were preventable. Health authorities are reminding people who get the shot to keep the spot where they were inoculated covered and to avoid touching the skin and the bandages that cover it. Even people who have not been vaccinated can become ill if they touch the inoculation site of someone who was. **Both women are recovering and not expected to have permanent scars. This brings to three the number of moderate-to-severe reactions among civilians as a result of smallpox vaccinations.** Last week, the CDC reported that a 39-year-old Florida nurse appeared to have a rash called generalized vaccinia.  
Source: [http://boston.com/dailynews/065/wash/Two\\_women\\_not\\_vaccinated\\_for\\_smallpox.html](http://boston.com/dailynews/065/wash/Two_women_not_vaccinated_for_smallpox.html)
14. *March 07, Reuters* — **Dutch chicken workers to get flu jabs. Dutch health officials said on Friday that people working with chickens involved in an outbreak of bird flu would be vaccinated against human influenza, to avoid the slim chance of the human and bird viruses combining into a strain dangerous to humans.** "This is the standard flu vaccine which we give every autumn," a ministry of health spokesman Bas Kuyk told Reuters Health. "What we want to do is exclude that possibility that H7N7 (bird) virus will combine itself with a human flu, then we have what is going on in Hong Kong." **Up to 25 farms in a small area in the center of the Netherlands have been identified as possibly or definitely infected with the bird virus in the first outbreak of the disease in Holland since 1926.**  
Source: <http://asia.reuters.com/newsArticle.jhtml?type=healthNewsoryID=2343841>
15. *March 06, Washington University School of Medicine* — **New mouse virus may help scientists better understand cruise ship epidemics.** A close relative of a common little-understood human virus that causes an estimated 23 million episodes of intestinal illness, 50,000 hospitalizations, and 300 deaths each year has been discovered in mice. **Discovery of the new virus, known as murine norovirus 1 (MNV-1), may lead to a better understanding of its disease-causing cousins known as Norwalk viruses, or human noroviruses (HNVs). HNVs cause 90 percent of epidemic viral gastroenteritis worldwide, including those that sweep through cruise ships, nursing homes, and military**

**encampments causing debilitating diarrhea and vomiting.** "We know very little about human noroviruses because they cannot be grown in the laboratory or in animals," says study leader Herbert W. Virgin IV, M.D., Ph.D., professor of pathology and immunology and associate professor of molecular microbiology. **"This new mouse virus will for the first time allow us to study this important class of human pathogens."**

Source: <http://aladdin.wustl.edu/medadmin/PANews.nsf/news/AE60E8F4D53C2B8C86256CE0005DBB1D?OpenDocument>

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

## Government Sector

16. *March 07, New York Times* — **\$60 million package aims to improve school security.** The Bush administration is stepping up federal efforts to prepare the nation's schools for possible terrorist strikes and is about to announce a \$60 million program to help school districts design response and evacuation plans for emergencies including chemical or biological attacks, administration officials said Friday. **The officials said the program was not meant to suggest that the government believed that schools faced a special threat from terrorists. They said instead that it was an effort to make sure that schools were as well prepared as other public and private places.** A model emergency response plan that is expected to be released by the Education Department encourages schools, public and private alike, to develop a plan that "addresses traditional crises and emergencies such as fires, school shootings and accidents, as well as biological, radiological, chemical and other terrorist activities." **It urges schools to conduct a safety assessment of their buildings, including their proximity "to rail tracks that regularly transport hazardous materials or facilities that produce highly toxic material."** The department also has a Web site for planning help: [www.ed.gov/emergencyplan](http://www.ed.gov/emergencyplan).

Source: <http://www.nytimes.com/2003/03/07/politics/07HOME.html>

17. *March 06, Associated Press* — **Terror threat could close tourist sites.** Some of the country's most popular tourist sites might be closed temporarily if a war with Iraq raises new terrorist concern. **The Statue of Liberty, the Washington Monument, the White House, the St. Louis Gateway Arch and the Liberty Bell pavilion in Philadelphia would probably be temporarily sealed off, Interior Department officials said Thursday.** "The National Park Service is prepared to take the appropriate action, as we have in the past, to protect public safety and preserve these monuments and memorials," spokesman Dave Barna said. The Interior Department has been developing emergency plans over the past five years, first for the millennium and then for homeland security after the September 11, 2001 terrorist attacks. **Also on the government's priority list for protection is Mount Rushmore in South Dakota. The Park Service already has increased patrols and guards at 11 more of the 388 areas it manages, primarily those that share borders with Canada or Mexico, or at seashores.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A52557-2003Mar 6.html>

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

## Emergency Services Sector

18. *March 07, Washington Post* — **Bomb hoax empties part of capitol.** Police said they will review security procedures at the U.S. Capitol, after a man and a woman walked through a screening area there Thursday while hiding objects duct-taped to their bodies. The incident prompted the evacuation of part of the Capitol for about an hour. **Police did not notice the two, who had Senate Gallery passes, until they reached an area near the center of the Capitol about 1:15 p.m. Officers, thinking the two had suicide bombs, began evacuating nearby offices. Police later concluded that the devices were a hoax and arrested the pair.** U.S. Capitol Police Chief Terrance W. Gainer said the two passed through the security post wearing baggy clothes and without setting off metal detectors. "I suspect there could be some minor adjustments" in security precautions, Gainer said, declining to elaborate on what those changes might be. "We still need to balance the need to access the Capitol and not be overbearing, [while] trying to live in terroristic times." **Ilelabayo David Olaniyi, 32, and Rena Patel, 22, were charged with interstate transportation of an explosive device, Gainer said. He added that the count can be used in the case of a hoax.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A54244-2003Mar 6.html>

19. *March 07, Milwaukee Journal Sentinel* — **15 live bombs found in house after explosion; man critically injured.** More than a dozen live bombs and a cache of bomb-making materials discovered at an apartment Hartford, WI after an explosion that critically injured a 33-year-old man, authorities reported on Friday. The man was building a bomb when the explosion occurred, Hartford Police Chief Thomas Jones said. **The 15 live bombs, discovered in crates taken from the apartment, a storage area and a garage in the 700 block of Grand Ave., had price tags affixed to them, Jones told a reporter. Members of the police department and federal agents discovered the items just before noon Friday. Police and fire units responded to reports of the explosion about 6:15 p.m. Thursday.** Residents were evacuated from a one-block area, which included several apartment buildings. The American Red Cross was called in and worked with residents until they were allowed to return to their homes about 2 a.m., Jones said. The front window of the apartment was blown out by the force of the explosion, which was heard blocks away – including by a police officer outside his home, Jones said. "What his intent was, we have no idea at this point," Jones said. "Until we delve deeper into his life, we cannot answer that question."

Source: <http://www.jsonline.com/news/ozwash/mar03/123552.asp>

20. *March 07, Las Vegas Review-Journal* — **Southern Nevada to stage bioterror test as part of national drill.** A lethal bioterror attack on the Strip is one scenario set for a nationwide training exercise in August. **The simulated pneumonic plague attack on Las Vegas will be done at Indian Springs Air Force base, 45 miles northwest of the city, and involve 3,000 to 5,000 people locally who work for federal, state and local governments. The nationwide anti-terror exercise, coordinated by the Defense Department, will test whether the nation's pharmaceutical stockpile is capable of handling biological and chemical attacks. President Bush and a number of state governors are set to participate.** "The governor literally will be asking the president for help," said Jerry Bussell, homeland security adviser to Gov. Kenny Guinn. "They will fly in emergency packages with medicine, food and clothing. We want to test all of those procedures." Domestic security officials at all levels of government have been planning since the fall for the Aug. 18-29 drill.

Source: [http://www.reviewjournal.com/lvrj\\_home/2003/Mar-07-Fri-2003/](http://www.reviewjournal.com/lvrj_home/2003/Mar-07-Fri-2003/)

[news/20835179.html](http://news/20835179.html)

21. *March 07, Department of Homeland Security* — **Department of Homeland Security announces funding for first responders. Secretary of Homeland Security Tom Ridge announced on Thursday that nearly \$600 million has been made available to the states and U.S. territories to better assist state and local public safety and law enforcement personnel in preventing, preparing for and responding to terrorism.** Secretary Ridge wrote to the Governors of the states and territories on Monday, March 3 to provide program guidelines and offer instructions for filing the grant applications. **Application forms for grant awards will be posted on the web at [www.ojp.usdoj.gov/fundopps.htm](http://www.ojp.usdoj.gov/fundopps.htm) by Friday, March 7 and states will have until April 22, 2003 to complete and submit their applications. Once the application is submitted, a review will be completed and the states will be notified of the status within 7 days. When approved, funds will be available within three weeks thereafter.** For a breakdown of funding by state, view the ODP grants chart.  
[http://www.dhs.gov/interweb/assetlibrary/ODP\\_State\\_Homeland\\_Security\\_Grant\\_Program.pdf](http://www.dhs.gov/interweb/assetlibrary/ODP_State_Homeland_Security_Grant_Program.pdf)  
Source: <http://www.dhs.gov/dhspublic/display?content=500>

[[Return to top](#)]

## **Information and Telecommunications Sector**

22. *March 05, CNET News* — **Net consortium ties flaws to BIND. Domain name servers are used to match domain names to numerical Internet Protocol addresses. As the vast majority of these run BIND (Berkeley Internet Name Domain), the software essentially runs the Internet.** The Internet Software Consortium (ISC), the group responsible for maintaining the software, released a new version of BIND on Monday, with their Web site billing it as a maintenance release. However, on Wednesday the site had been updated, saying that **the ISC had been made aware of vulnerabilities in BIND, adding that upgrading was "strongly recommended."** BIND 9.2.1 is vulnerable to a remote buffer overflow bug when installed with the "libbind" nondefault option. Previous versions may also be vulnerable to problems associated with the commonly used OpenSSL library, but again this is a nondefault installation option and has more to do with the SSL library than BIND itself. An updated version of BIND is available at the ISC website: <http://www.isc.org/products/BIND/>.  
Source: <http://news.com.com/2100-1032-991123.html>
23. *March 05, SecurityFocus* — **Windows root kits a stealthy threat. A Windows root kit called "ierk8243.sys" was discovered on the network of Ontario University last January. It has since been dubbed "Slanret", "IERK," and "Backdoor-ALI." A root kit is an assembly of programs that subverts the Windows operating system at the lowest levels, and, once in place, cannot be detected by conventional means.** Also known as "kernel mode Trojans," root kits are far more sophisticated than the usual batch of Windows backdoor programs. Greg Hogle, a California computer security consultant, believes intruders have been using Windows root kits covertly for years. He says the paucity of kits captured in the wild is a reflection of their effectiveness -- not slow adoption by hackers. Once Slanret is installed on a hacked machine, anti-virus software won't pick it up in a normal disk scan. That said, the program is not an exploit -- intruders have to gain access to the computer through some other means before planting the program. Despite their increasingly sophisticated design, the current

crop of Windows root kits are generally not completely undetectable, and Slanret is no exception. Because it relies on a device driver, booting in "safe mode" will disable its cloaking mechanism, rendering its files visible. And in what appears to be an oversight by the kit's author, the device driver "ierk8243.sys" is visible on the list of installed drivers under Windows 2000 and XP, according to anti-virus company Symantec Security Response. Hoglund says future Windows root kits won't suffer from Slanret's limitations. And while he says the risk can be reduced with smart security policies -- accept only digitally-signed device drivers, for one -- ultimately, he worries the technique may find its way into self-propagating malicious code.

Source: <http://www.securityfocus.com/news/2879>

### Internet Alert Dashboard

| Current Alert Levels                                                                                                                                                 |                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br>AlertCon: 2 out of 4<br><a href="https://gtoc.iss.net">https://gtoc.iss.net</a> | <br>Security Focus ThreatCon: 1 out of 4<br><a href="http://analyzer.securityfocus.com/">http://analyzer.securityfocus.com/</a>                                                            |
| Current Virus and Port Attacks                                                                                                                                       |                                                                                                                                                                                                                                                                              |
| <b>Virus:</b>                                                                                                                                                        | #1 Virus in the United States: <b>WORM_KLEZ.H</b><br>Source: <a href="http://wtc.trendmicro.com/wtc/wmap.html">http://wtc.trendmicro.com/wtc/wmap.html</a> , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States] |
| <b>Top 10 Target Ports</b>                                                                                                                                           | 80 (www), 137 (netbios-ns), 1434 (ms-sql-m), 445 (microsoft-ds), 135 (epmap), 139 (netbios-ssn), 25 (smtp), 113 (ident), 53 (domain), 0 (----)<br>Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center      |

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

## General Sector

**24. March 07, Reuters** — **Hong Kong extradites three to U.S. in al Qaeda case.** Hong Kong has extradited three men to the United States, where they are wanted for allegedly trying to buy anti-aircraft missiles for al Qaeda, a government spokeswoman said on Friday. "They arrived in the U.S. this morning," she added. **The three -- two Pakistanis and a U.S. citizen of Indian origin -- had been in custody in Hong Kong since September after they were arrested for allegedly trying to sell a huge haul of heroin and hashish to undercover FBI agents in exchange for four Stinger missiles. The Hong Kong government said the men -- Syed Saadat Ali Faraz, Muhammed Abid Afridi and Ilyas Ali -- had intended to deliver the Stingers, which can destroy low-flying planes, to al Qaeda.** The trio had originally wanted to fight the extradition order, but later changed their minds. The reason was not known. Source: <http://www.washingtonpost.com/wp-dyn/articles/A54718-2003Mar 7.html>

## **NIPC Products & Contact Information**

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC 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 NIPC web-site (<http://www.nipc.gov>), one can quickly access any of the following NIPC products:

[NIPC Warnings](#) – NIPC Assessments, Advisories, and Alerts: The NIPC produces three levels of infrastructure warnings which are developed and distributed consistent with the FBI's National Threat Warning System. 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.

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

[NIPC Daily Reports Archive](#) – Access past NIPC Daily Reports

### **NIPC Daily Open Source Report Contact Information**

Content and Suggestions: [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) or contact the NIPC Daily Report Team at 202-324-1129

Distribution Information Send mail to [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) for more information.

### **Contact NIPC**

To report any incidents or to request information from NIPC, contact the NIPC Watch at [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov) or call 202-323-3204.

### **NIPC Disclaimer**

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