Department of Homeland Security
Daily Open Source Infrastructure Report
for 21 August 2007

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- Symantec Corp. reports a new Trojan horse called Infostealer.Monstres has stolen more than 1.6 million records belonging to several hundred thousand people from Monster Worldwide Inc.'s job search service, setting them up for phishing mail that plants malware on their machines. (See item 4)

- The Associated Press reports Texas officials opened emergency operations centers, moved inmates to prisons deeper inland, and passed out sandbags along portions of the Texas coast as Hurricane Dean barrels toward the warm waters of the Gulf of Mexico. (See item 18)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

---

Energy Sector

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

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

1. *August 20, Associated Press* — **Pascagoula Chevron refinery operates after fire.** Chevron's largest U.S. refinery continued production Friday, August 17, while teams assessed damage caused by a fire Thursday in one section of the sprawling facility. "We have teams together that are investigating both the root cause of the incident as well as assessing the extent of the damage and putting together a repair plan," said Steve Renfroe, a spokesperson at Chevron's Pascagoula plant. Renfroe said he didn't know when the reports about damage and a possible cause would be available. He said other areas of the plant continued to operate. The refinery

employs 1,350 people. Meanwhile, Renfroe said Chevron officials were monitoring Hurricane Dean, which the National Hurricane Center said Friday had strengthened to a Category 3 storm with 125 mile−an−hour winds The facility is one of the top 10 petroleum refineries in the United States and has been operating on the Mississippi coast since 1963.
Source: http://biz.yahoo.com/ap/070817/chevron_fire_investigation.ht ml?.v=1

2. *August 20, Associated Press* — **Mexico abandons oil rigs ahead of Dean.** Hurricane Dean headed for a collision course with Mexico's Yucatan Peninsula on Monday, August 20, forcing the state−run oil company to abandon its off−shore rigs. The storm killed 10 people as it crossed the Caribbean. Dean was already a powerful Category 4 storm as it raked the Cayman Islands. The U.S. National Hurricane Center said it could grow into a monstrous Category 5 hurricane before slashing across the Yucatan Peninsula and emerging in the oil−rich Gulf of Campeche. Mexico's state oil company decided Monday to evacuate all 14,000 workers and shut down production on the offshore rigs that extract most of the nation's oil.
Source: http://www.abcnews.go.com/International/wireStory?id=3501735

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *August 20, Associated Press* — **Crews race rain to neutralize sulfuric acid spill.** Emergency response crews beat an approaching storm to neutralize about 100 gallons of sulfuric acid spilled on a highway in Romney, IN, before rain turned it into a toxic gas. Minutes before the storm arrived on Sunday, August 19, crews neutralized the acid with a sodium−based substance, eliminating the need to evacuate nearby residents. About 100 gallons of sulfuric acid spilled at the intersection of U.S. 231 and Indiana 28 when a semi−truck's pressure relief valve popped off. Police closed sections of Indiana 28 near Romney about 10 miles south of Lafayette as a precaution. They alerted nearby residents that they might be evacuated if rain water had caused a chemical reaction and produced a toxic gas.
Source: http://www.wave3.com/Global/story.asp?S=6955186&nav=menu31_3

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *August 19, ComputerWorld* — **Identity attack spreads; 1.6 million records stolen from Monster.com.** The 46,000 people reportedly infected by ads on job sites may be only a fraction of the victims of an ambitious, multistage attack that has stolen data belonging to several hundred thousand people who posted resumes on Monster.com, a researcher said this past weekend. According to Symantec Corp. security analyst Amado Hidalgo, a new Trojan horse called Infostealer.Monstres by Symantec has stolen more than 1.6 million records belonging to

several hundred thousand people from Monster Worldwide Inc.'s job search service. That data is then used to target the Monster.com users with credible phishing mail that plants more malware on their machines. The personal information filched from Monster.com includes names, e−mail addresses, home address, phone numbers and resume identification numbers, said Hidalgo, who traced the data to a remote server used by the attackers to store the stolen information. Infostealer.Monstres ripped off Monster.com by using legitimate log−ins, likely stolen from recruiters and human resource personnel who have access to the "Monster for employers" areas of the site.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9031418&intsrc=hm_ts_head

5. *August 18, IDG News Service* — **Phishers can misuse Google Gadgets.** The domain used to host small Google Gadget applications written by Web developers could be misused by phishers, according to Robert Hansen, a Web security researcher. Google Gadgets are little programs that gather information on the Web and then display them on multiple Web pages. They are used to give Webmasters an easy way to display everything from sports scores to astronomical data on their sites. Unfortunately, they can also be misused by phishers to get around antiphishing filters. Attackers could create a phishing site on the gmodules.com domain and then send that URL to victims. Because Google's gmodules.com domain is trusted by antiphishing filters, victims might then go to the phishing site without being warned by their browser's filtering software.
Source: http://news.yahoo.com/s/pcworld/20070818/tc_pcworld/136129;_ylt=AogHmWHs7XtbXoyYM84vP6gjtBAF

6. *August 17, Reuters* — **SEC charges ex−Brocade CFO in backdating scheme.** The U.S. Securities and Exchange Commission (SEC) charged Brocade Communications Systems former chief financial officer (CFO) with fraud on Friday, August 17, saying he disregarded indications other executives were backdating stock options. The SEC said Michael Byrd learned of instances in which Brocade's former CEO and others were backdating options for certain people, but did not ensure the company properly accounted for the expenses and disclosed them to investors. A U.S. jury convicted the former Brocade CEO Gregory Reyes earlier this month in the government's first criminal trial of options backdating. Brocade has already agreed to pay a $7 million civil penalty to settle charges of fraudulent stock option backdating. The SEC said Reyes repeatedly granted "in−the−money" options to employees and executives, but signed backdated grant paperwork to avoid reporting significant expenses. The agency also said Byrd received a backdating option grant in 2001, and filed a disclosure statement with the SEC with a false grant date.
Source: http://news.com.com/SEC+charges+ex−Brocade+CFO+in+backdating+scheme/2100−1014_3−6203251.html

[Return to top]

Transportation and Border Security Sector

7. *August 20, CNN* — **All safe after fire guts airliner.** A Taiwanese jetliner burst into flames Monday, August 20, shortly after landing at the Naha airport on the Japanese island of Okinawa, but 165 passengers and crew got off the plane safely, authorities said. The Japanese

Transport Ministry and the Naha Fire Department said the passengers included 155 adults and two toddlers. The crew was made up of two pilots and six flight attendants. According to the ministry, there was "some sort of explosion" on board the China Airlines Boeing 737, but no other details were immediate available. Japanese media reported that a passenger saw a fire in one of the engines before the blast. This incident is the latest in a series of accidents involving China Airlines. Jetliners for the air carrier crashed in 2002, 1999, 1998 and 1994, killing more than 1,000 people.
Source: http://www.cnn.com/2007/WORLD/asiapcf/08/20/japan.plane/inde x.html

8. *August 20, Russia Today* — **Russia tightens air safety rules.** Starting August 27, Russia is introducing stricter security checks before and after flights, along with new limits on the size and contents of hand luggage. "We are changing the rules to bring them in line with the latest rules on air safety and to meet the requirements introduced by the International Civil Aviation Organization (ICAO). All our regulations regarding liquids, gels, and so on, literally repeat the instructions sent to us by the ICAO," Vladimir Chertok, air traffic official, said.
Source: http://www.russiatoday.ru/news/news/12740

9. *August 19, Wall Street Journal* — **Small jets, big problems: Airport delays on the rise.** The nation's air–travel system approached gridlock early this summer, with more than 30 percent of June's flights late by an average of 62 minutes. The mess revved up a perennial debate about whether billions of dollars should be spent to modernize the air–traffic–control system. But one cause of airport crowding and flight delays is receiving scant attention. Airlines increasingly carry passengers into jammed airports on smaller airplanes. That means using more flights –– and increasing the congestion at airports and in the skies around them. Aircraft numbers indicate U. S. airlines grounded a net 385 large planes from 2000 through 2006 –– but they added 1, 029 regional jets –– according to data firm Airline Monitor. The small–plane conundrum is, at least in part, a byproduct of the financial troubles of the airline industry. After September 11, 2001, airlines grounded older, larger jets that were gas guzzlers. The big jets weren't needed when traffic dropped dramatically after the terrorist attacks. Now traffic is coming back. But many airlines have deployed most of the widebodies they have in international flying, which is more lucrative because it faces less price competition. Meanwhile, flight delays have worsened every year since 2003, according to the Bureau of Transportation Statistics.
Source: http://www.nwanews.com/adg/Business/199002/

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

10. *August 19, Agriculture Online* — **Southern Plains feral swine pose disease risks.** Swine producers work with pen design, housing construction and biosecurity measures to protect pigs

against feral hogs that can carry and transmit disease. And, there's no shortage of the wild pigs in Texas. Of the nearly three million swine in the state, more than two million are wild. The U.S. Department of Agriculture Wildlife Services in Texas submitted samples from nearly 700 wild swine from August 2003 through May 2007. Test results showed that more than 20 percent had pseudorabies, a highly contagious viral disease that can cause mild flu–like signs in sows and boars, or kill piglets. About 10 percent were positive for swine brucellosis, a bacterial infection that can cause sows to abort.
Source: http://www.agriculture.com/lcl/story.jhtml?storyid=/template data/ag/story/data/1187274486268.xml&catref=ag1001

11. *August 18, CNN* — **Mystery ailment kills hundreds of Saudi camels.** Hundreds of camels have died in Saudi Arabia from a mystery ailment. The Agriculture Ministry has said 232 camels died in the space of four days in the Dawasir Valley, 250 miles south of Riyadh. Agriculture ministry officials have denied an infectious disease caused the deaths and blamed them on animal feed supplied by food storage authorities.
Source: http://edition.cnn.com/2007/WORLD/meast/08/18/saudi.camels.r eut/?imw=Y&iref=mpstoryemail

12. *August 17, Garden Island (HI)* — **Banana bunchy top virus still an island–wide epidemic.** The banana bunchy top virus has spread throughout Hawaii and if not swiftly dealt with, may impede bananas from growing on island soil for years to come. The banana bunchy top virus first appeared on Kauai in 1997, eight years after it had first been observed on Oahu. Kauai farmers and Craig Kaneshige, the pest specialist at Kauai's Department of Agriculture, report the disease has come back and taken a strong hold. "My partner and I have recently seen diseased plants from Kalihiwai ridge to Hanapepe. Not only right off the road, but also deep inland. My partner went hiking into the valley, and spotted wild banana plants that are infected now." The prognosis for a disease of this magnitude is devastating. BBTV is spread by a vampire aphid that feeds on a plant and simultaneously infects it. Throughout its life span of 15–20 days the aphid will carry the disease as it moves from plant to plant, and once a plant is infected, a clean aphid can contract the disease just by feeding where the sickness already dwells. Banana plants that show symptoms rarely bear fruit.
Source: http://www.kauaiworld.com/articles/2007/08/18/news/news03.tx t

[Return to top]

Food Sector

13. *August 18, CanWest News Service (Canada)* — **Carrots recalled after four people get sick.** Consumers should not eat one brand of baby carrots sold recently at Costco stores because of contamination by shigella, which causes fever, nausea and vomiting, the Canadian Food Inspection Agency has warned. The carrots are labelled Los Angeles Salad Company Genuine Sweet Baby Carrots, and they come from Mexico. They were sold in British Columbia, Alberta, Ontario, Quebec and Newfoundland. Food is usually contaminated by shigella when it comes in contact with water polluted by human sewage.
Source: http://www.canada.com/topics/news/national/story.html?id=101 e934e–7f3f–46e3–8193–2ec04a24c853&k=75341

14. *August 18, Washington Post* — **Import safety panel points to technology.** Improving the safety of U.S. imports will require boosting the quality of the manufacturing process and expanding the use of technology, two members of a presidential working group said Friday, August 17. They said, however, that improvement cannot be accomplished through blanket inspections. "We will not be able to inspect our way to food and product safety," said Mike Leavitt, secretary of Health and Human Services and chairman of the panel. "The scale makes it impossible to inspect everything." He predicted that imports would increase threefold by 2015. The group's strategic plan, to be issued next month, will include measures to improve safety by boosting manufacturing quality, using technology to inspect more goods at ports rather than in faraway labs and ensuring that exporting countries understand U.S. safety standards, Leavitt said. The Department of Homeland Security will probably play an expanded role in improving the safety of food and products entering the country, said Michael Chertoff, the department's secretary. The working group is halfway through its review process, which has included visits to ports, food–processing centers and supermarkets.
Source: http://www.washingtonpost.com/wp–dyn/content/article/2007/08/17/AR2007081702191.html

15. *August 16, Food Safety and Inspection Service* — **FSIS launches Web feature to answer technical and policy questions.** The U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) Thursday, August 16, launched askFSIS, a new Web–based feature, designed to help answer technical and policy questions regarding inspection and public health regulations 24 hours a day. The new interactive feature will provide answers on technical issues in more depth than the standard list of "frequently asked questions" currently available through FSIS' Website. It will allow visitors to seek answers on topics such as exporting, labeling and inspection–related policies, programs and procedures. AskFSIS is designed to serve a business audience. "This new Web–based tool will be especially helpful for owners and operators of small and very small plants," said USDA Under Secretary for Food Safety Richard Raymond.
Source: http://www.fsis.usda.gov/News_&_Events/NR_081607_01/index.as p

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

16. *August 20, Agence France–Presse* — **Indonesia, Japan to cooperate on bird flu vaccine.** Indonesia has offered to cooperate with Japan in developing a human bird flu vaccine, President Susilo Bambang Yudhoyono said Monday, August 20, during a visit by Japanese Prime Minister Shinzo Abe. Yudhoyono said the pair had "agreed on cooperation in dealing with avian influenza" during talks in the Indonesian capital. "I have offered Prime Minister Abe bilateral cooperation in developing a human vaccine based on the Indonesian strain of the virus, for the sake of our welfare and the global interest," he said. Indonesia has been rapped by the

World Health Organization for failing to share its samples with the rest of the world, saying it will not formally hand more over until is guaranteed access to affordable medicines to treat victims.
Source: http://news.yahoo.com/s/afp/20070820/hl_afp/healthfluindones iajapan_070820072019;_ylt=AnQW7br8ILbMAbKblr.vt9WJOrgF

17. *August 16, Tric−City Herald (WA)* — **Health District confirms fifth hantavirus case.** A 65−year−old Franklin, WA, man is in intensive care in Seattle after being diagnosed earlier this week with Hantavirus Pulmonary Syndrome, a health official said Wednesday, August 15. The man is the fifth confirmed case of hantavirus in the Benton−Franklin Health District this year, and the third in the past week, according to Larry Jecha, the Benton−Franklin Health District medical director. The district usually doesn't hear of more than one case of hantavirus per year, Jecha said, so the health district has warned local health service providers to be on the lookout for symptoms. The two other cases reported this week were family members, women ages 45 and 24. They also are from the Benton−Franklin county area. The 24−year−old was admitted to an area hospital Tuesday, Jecha said, while the other woman was treated at a hospital and released. Two other cases were reported in the area in June, Jecha said, adding that the rest of the state has not reported any incidents of the virus this year.
Source: http://www.tri−cityherald.com/tch/local/story/9224381p−91403 40c.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

18. *August 20, Associated Press* — **Texas prepares for Hurricane Dean.** Officials opened emergency operations centers, moved inmates to prisons deeper inland, and passed out sandbags along portions of the Texas coast as Hurricane Dean barreled toward the warm waters of the Gulf of Mexico. Dean was several days away and its path was still uncertain, but officials weren't taking any chances. Even if the hurricane continues a steady westward course toward Mexico, parts of the already saturated state could be flooded by the storm's outer bands. As of 8:00 a.m. EDT Monday, August 20, Dean was about 440 miles east of Belize City and was traveling west at near 21 mph, the National Hurricane Center said. With Dean on the way, officials in Cameron County, at Texas' southern tip, opened emergency operations centers and urged residents to evacuate ahead of the storm. Texas Governor Rick Perry mobilized the National Guard and search−and−rescue teams, shipped 60,000 to 80,000 barrels of gasoline to gas stations in the Rio Grande Valley, and got a pre−emptive federal disaster declaration from President Bush. The state also sent six C−130 aircraft to Cameron County in case any critically ill patients needed to be evacuated. Hundreds of buses were on standby for possible evacuations.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/08 /20/AR2007082000312.html

19. *August 20, The Day (CT)* — **Regional emergency dispatch possible with latest technology.** Recent and planned upgrades to the emergency dispatch center in Waterford, CT, will catapult the town into the forefront of Connecticut first–responder communications. The upgrades put Waterford in a position to become a central hub of a regional emergency dispatch system for surrounding municipalities such as East Lyme, Montville and New London, offering better communication in times of trouble and probably saving taxpayers some money. It could be a contender, that is, if communities decide a central hub makes sense, and that's the topic of a regional discussion that is just beginning. "The technology is there," said Wayne Sanford, deputy commissioner of the state Department of Emergency Management and Homeland Security. "The hard part is getting everyone to buy into it." Regionalization requires a great deal of cooperation from all communities involved, and overcoming the inertia of municipal government is not an easy task. "It's definitely in sync with the direction our agency is going," Sanford said. Regionalization of emergency dispatch provides "a better level of service, especially when there are multiple incidents going on at the same time."
Source: http://www.theday.com/re.aspx?re=45c9f387–931d–420a–9863–24c d86524351

[Return to top]

Information Technology and Telecommunications Sector

20. *August 20, IDG News Service* — **RF Micro to buy Sirenza in $900 million deal.** Mobile phone chip maker RF Micro Devices plans to buy Sirenza Microdevices in a $900 million deal aimed at expanding its presence in WiMax, broadband, cable TV, and wireless infrastructure. The deal is a sign that merger and acquisition activity in the technology sector is not over, despite credit industry problems that have roiled global stock markets.
Source: http://www.infoworld.com/article/07/08/20/RF–Micro–to–buy–Si renza_1.html

21. *August 17, Websense Security Labs* — **Malicious Website/Malicious Code: Biotechnology Information Organization site compromise.** Websense Security Labs has discovered that the official site of the Biotechnology Industry Organization (www.bio.org) has been compromised and infects visitors with a malicious script that attempts to exploit multiple vulnerabilities. The Biotechnology Industry Organization's Website is commonly visited by members of the biotech industry. To date Websense has seen infected pages only within the news and public relations sections of their site. This same exploit is used by the people behind the attack on Syndicate Bank of India.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=795

<div align="center">

Internet Alert Dashboard

</div>

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

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

22. *August 20, Associated Press* — **Investigators probe New York skyscraper fire.** Authorities are investigating the cause of a fire that killed two firefighters in a condemned ground zero skyscraper where conditions were stacked against the responders at every turn. Officials said the fire was not believed to be electrical and that crews dismantling the building before the flames broke out on Saturday, August 18, had not been working with torches. Fire marshals could not even enter the building until Sunday because small pockets of fire were still burning, but they had been questioning witnesses, including an elevator operator who first reported the blaze. Investigators also were interested in graffiti on a work shed that made reference to a burning building, authorities said. Fire Department of New York spokesperson Frank Gribbon said the fire has not been deemed suspicious; authorities have not ruled out every accidental cause. High−rise fires are always treacherous, but the firefighters who responded to the abandoned ground zero skyscraper faced a series of unforeseen complications: the main water supply failed, the fire was difficult to reach, and the condemned 41−story building was thought to pose health risks to emergency responders and the neighborhood.
Source: http://hosted.ap.org/dynamic/stories/D/DEUTSCHE_BANK_FIRE?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

23. *August 19, Post Chronicle (CA)* — **RPG live round discovered in stolen California van.** A Marine Corps bomb unit was called in by California police who found an Iraqi−style rocket propelled grenade stashed in a stolen van. The weapon was detonated Friday, August 17, inside the vehicle, which had been reported stolen a few weeks ago and had just been returned to its owner. Ernie Adkins of Laguna Niguel, CA, was inspecting his newly returned customized Ford E350 van when he found the weapon in the overhead rack. Orange County bomb squad deputies summoned Marines from nearby Camp Pendleton, who likely had a lot more experience with the weapons known as RPGs, a favorite of Iraqi insurgents.
Source: http://www.postchronicle.com/news/strange/article_21298436.s html

[[Return to top]]

General Sector

Nothing to report.
[[Return to top]]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport