



**TAKE A SURVEY**

RESEARCH PURPOSES ONLY



[Back to article](#)  [Print this](#)

## Hackers launch major attack on U.S. military labs

# Sophisticated cyber attacks break into computer systems at the U.S. military's Oak Ridge National Laboratory in Tennessee and Los Alamos National Laboratory in New Mexico

By John E. Dunn, Techworld.com, IDG News Service

December 07, 2007

Hackers have succeeded in breaking into the computer systems of two of the United States' most important science labs, the Oak Ridge National Laboratory (ORNL) in Tennessee and Los Alamos National Laboratory in New Mexico.

In what a spokesperson for the Oak Ridge facility described as a "sophisticated cyber attack," it appears that intruders accessed a database of visitors to the Tennessee lab between 1990 and 2004, which included their Social Security numbers and dates of birth. Three thousand researchers reportedly visit the lab each year, a who's who of the science establishment in the United States.

The attack was described as being conducted through several waves of phishing e-mails with malicious attachments, starting on Oct. 29. Although not stated, these would presumably have launched Trojans if opened, designed to bypass security systems from within, which raises the likelihood that the attacks were targeted specifically at the lab.

ORNL director, Thom Mason, described the attacks in an e-mail to staff earlier this week as being a "coordinated attempt to gain access to computer networks at numerous laboratories and other institutions across the country."

"Because of the sensitive nature of this event, the laboratory will be unable for some period to discuss further details until we better understand the full nature of this attack," he added.

The ORNL has set up a Web page giving an official statement on the attacks, with advice to employees and visitors that they should inform credit agencies so as to minimize the possibility of identity theft.

Less is known about the attacks said to have been launched against the ORNL's sister-institution at Los Alamos, but the two are said to be linked. It has not been confirmed that the latter facility was penetrated successfully, though given that a Los Alamos spokesman said that staff had been notified of an attack on Nov. 9 -- days after the earliest attack wave on the ORNL -- the assumption has to be that something untoward happened there as well, and probably at other science labs across the United States.



The ORNL is a multipurpose science lab, a site of technological expertise used in homeland security and military research, and also the site of one of the world's fastest supercomputers. Los Alamos operates a similar multidisciplinary approach, but specializes in nuclear weapons research, one of only two such sites doing such top-secret work in the United States.

Los Alamos has a checkered security history, having suffered a sequence of embarrassing breaches in recent years. In August of this year, it was revealed that the lab had released sensitive nuclear research data by e-mail, while in 2006 a drug dealer was allegedly found with a USB stick containing data on nuclear weapons tests.

"This appears to be a new low, even drug dealers can get classified information out of Los Alamos," Danielle Brian, executive director of the Project On Government Oversight (POGO), said at the time. Two years earlier, the lab was accused of having lost hard disks.

The possibility that the latest attacks were the work of fraudsters will be seen by some as optimistic -- less positive would be the possibility of a rival government having been involved. Given the apparently coordinated nature of events, speculation will inevitably point to this scenario, with the data theft a cover motivation for more serious incursions.

*Techworld is an InfoWorld affiliate.*

 [Print this](#)