Top US government research labs infiltrated by hackers

By Ryan Paul | Published: December 09, 2007 - 01:21PM CT

http://arstechnica.com/news.ars/post/20071209-top-us-military-research-labs-infiltrated-by-hackers.html

Hackers successfully infiltrated Oak Ridge National Laboratory (ORNL), one of the nation's leading government-run research facilities. The attackers gained access by sending e-mails infected with trojan horses to ORNL employees. The lab claims that no classified information was retrieved, but admits that the perpetrators managed to acquire a database containing personal information about ORNL visitors and employees, including Social Security numbers.

"A hacker illegally gained access to ORNL computers by sending staff e-mails that appeared to be official legitimate communications. When the employees opened the attachment or accessed an embedded link, the hacker planted a program on the employees' computers that enabled the hacker to copy and retrieve information," ORNL revealed in a statement. "No classified information was lost; However, visitor personal information may have been stolen. If you visited ORNL between the years 1990 and 2004, your name and other personal information, such as your Social Security number or date of birth, may have been part of the stolen information."

ORNL believes that the intrusion was part of a larger coordinated attack on numerous research facilities in the United States. Representatives of Los Alamos National Laboratory (LANL) have acknowledged that an attack on their network took place last month, but ORNL is the only organization so far that has publicly confirmed an actual breach. A memo sent to LANL employees that was subsequently leaked to the public states that "malicious and determined hackers have accessed the Lab's unclassified Yellow Network and removed a significant amount of unclassified material."

LANL and ORNL were originally constructed during during World War II for highly sensitive nuclear weapons research. Today, the two facilities are used for research in numerous areas including national security, nanotechnology, advanced materials, and energy.

The identity of the hackers is not known, but some speculate that it was orchestrated by a foreign government. Various countries have recently detected widespread cyber attacks from from computers inside of China.

Although certain foreign governments are suspects, the attack could have been planned and carried out by almost anybody. It doesn't really take much to infiltrate highly secure facilities in the United States. Consider hacker Gary McKinnon, the self-described "bumbling computer nerd," who infiltrated almost 100 servers owned by the Defense Department, Navy, Army, Air Force, and other government agencies back in 2002 while looking for evidence of a UFO cover-up. McKinnon executed what the government describes as the biggest military computer hack on record and he did it with little more than a brute-force Perl script.

These recent attacks reflect the vulnerability of technological infrastructure in the United States and demonstrate the clear need for better security standards. Trojan horses should not be able to worm their way into military research facilities.