

Lab halts Web access after cyber attack

By Frank Munger

Tuesday, April 19, 2011

OAK RIDGE — A highly sophisticated cyber attack — known as Advanced Persistent Threat — forced Oak Ridge National Laboratory to shut down all Internet access and email systems over the weekend.

Those restrictions will remain in place until lab officials and others investigating the attack are sure the situation is well controlled and manageable, ORNL Director Thom Mason said Monday.

Mason said he expects that email functions may be restored today on a limited basis, with no attachments allowed and restrictions on length.

“We made the decision (at about midnight Friday) to close down the connection to the Internet to make sure there was no data exfiltrated from the lab while we got the system cleaned up,” he said.

The lab’s cyber specialists had been monitoring the attack and recommended further action after it looked like efforts were under way to remove data from ORNL systems, Mason said.

Mason said the APT threat at ORNL is similar to attacks in recent times on Google, a security company known as RSA and other government institutions and corporations.

“In this case, it was initiated with phishing email, which led to the download of some software that took advantage of a ‘zero day exploit,’ a vulnerability for which there is no patch yet issued,” he said. The vulnerability involved Internet Explorer, he said.

Mason said the lab has not, to this point, detected any large-scale exfiltration of data, and the decision to shut down Internet access was made to prevent that or anything similar to a 2007 cyber attack at ORNL in which large amounts of data were stolen. Following that event, the lab sent 12,000 letters to former lab visitors, informing them that their Social Security numbers may have been compromised (although there were no subsequent reports of identity thefts or major problems).

“We haven’t really completed the post-mortem on what happened, so it would be foolish to kind of speculate on where things were going,” Mason said, when asked about a report that the attack may have originated in China.

“There was no significant exfiltration of data that we detected,” he said. “There were attempts and small volumes of things that were suspicious in terms of Internet traffic.”

ORNL has solicited help from throughout government, including other Department of

Energy labs. He confirmed that some outside experts had arrived in Oak Ridge to participate in the investigation.

In addition, he said virtually all of the lab's information technology staff (about 200 people) was involved, either in the investigation or maintaining the functionality of internal systems.

Mason confirmed that some computers were confiscated and quarantined. He also confirmed that the phishing email messages in this case were disguised as coming from the lab's human resource department.

He said that some lessons learned from the 2007 attack helped lab officials with the current situation, but he said this is a much more advanced attack than the event four years ago.

"Well, if you look at this APT, it is much more sophisticated than what was being used a few years ago," he said. "Certainly what we've seen is very consistent with the RSA attack. ... Whoever is doing this attempts to get a foothold in the network system, works patiently and relatively quietly to try to expand that and is looking for specific types of information."

Without email or Internet access, thousands of ORNL employees weren't able to do business as usual on Monday.

"It hampered our normal communications," said Mason, who was out of town and could not check his email. "It means we're dusting off some fax machines."

Senior writer Frank Munger may be reached at 865-342-6329.



© 2011 Scripps Newspaper Group — Online