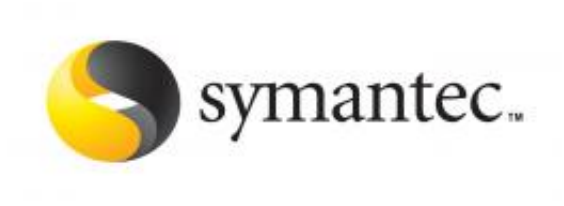
Indian hacker lords have Symantec antivirus code

January 7 2012, by Nancy Owano



(PhysOrg.com) -- An Indian hacker group called The Lords of Dharmaraja has laid claim to Symantec's antivirus software code. Symantec, confirming the theft in an e-mail posted Friday, said the chunk of pilfered code was stolen from a third party, was old, and that its own network had not been breached. The group had announced they got the code and confidential information. "Symantec can confirm that a segment of its source code used in two of our older enterprise products has been accessed, one of which has been discontinued," according to a spokesman for Symantec.

The stolen code is four to five years old and the Mountain View, California, company stressed that the there were no signs that customer information had been tampered with, and they stated that their own security networks had not been breached.

The Lords of Dharmaraja say they took the files from Indian military

intelligence servers.

A hacker from the group, Yama Tough, provided security site Infosec Island with files that appeared to contain source code from the 2006 version of Norton Antivirus. The site passed the code on to Symantec, which confirmed that the code was genuine. Symantec also pointed out that the exposed source code corresponded to its enterprise products.

Outside Symantec, reports said that the hackers gained access to source code related to Symantec Endpoint Protection (SEP) 11.0 and Symantec Antivirus 10.2; both were reportedly sitting on the Indian military servers. The Symantec Antivirus 10.2 was five years old and was discontinued but, according to Reuters, is still being serviced. SEP 11.0, utilized to block outgoing data from being leaked, was four years old and had been updated regularly since.

Security experts outside the company appear to concur with Symantec that the incident is unwelcome but not catastrophic. Fundamentally, the reaction was that there was not much the hackers could do with what they got.

“As someone who worked in the industry, I don't see a tremendous security risk to the source code release itself,” said contributor Kevin McAleavey, architect of the KNOS secure operating system and antimalware researcher, in Infosec Island.

He said the code was pre-Vista, was not 64-bit compatible, and the newer safe functions were not in use. Looking the code over, he concluded that it was indeed “genuine Symantec source code from an ancient version of their antivirus,” but at the same time could only be looked upon “by us antimalware coders as a museum exhibit, not an actual threat."

While security watchers did not see any serious consumer risks, the question being asked is, whether it is trophy, museum piece, or act of breach, however termed, but at what enterprise-business price? Analysts say that any hacker publicity involving a security software company can never be an easy ride for the affected vendor.