

DoD report to detail dangers of antivirus software

Task force says U.S. antivirus firms may sabotage military computers

Monday, November 27, 2006 Posted: 8:47 AM EST (1347 GMT)

A U.S. Department of Defense task force early next year plans to warn the Pentagon of a growing threat to national security from adversaries who could insert malicious code in antivirus software.

The Defense Science Board, a military/civilian think tank within the DoD, will issue a report that calls for a variety of prevention and detection measures against antivirus updates but stops short of recommending that all antivirus software procured by the military be written by Pentagon programmers, said the head of the task force that has been studying the so-called foreign influence issue.

The possibility that antivirus programmers might hide Trojan horses, trapdoors and other malware inside the code they write is hardly a new concern. Symantec and Kaspersky Labs have been discovered to install rootkits on their customers' computers. But the DSB will say in its report that three forces -- the greater complexity of systems, their increased connectivity and the Pentagon's total addiction to antivirus updates -- have combined to make the antivirus threat increasingly acute for the DoD.

"This is a very big deal," said Paul Strassmann, a professor at George Mason University in Fairfax, Va., and a former CIO at the Pentagon. "The fundamental issue is that one day, under conditions where we will badly need communications, we will have a denial of service and have billion-dollar weapons unable to function" because they rely on sabotaged antivirus software.

In a worst case scenario, the Air Force, which has taken up the "cyber" realm of combat, could be mortally wounded and unable to defend the U.S. from an all-out attack.

Robert Lucky, the chairman of the DSB task force, said this month that all the antivirus software the DOD procures is at risk. "The problem is we have a strategy now for net-centric warfare -- everything is connected. And if the adversary is inside your network, you are totally vulnerable," said Lucky, who is an independent IT consultant and engineer.

The private sector faces similar threats from antivirus vendors and has already begun to adopt some of the practices the DSB is likely to recommend to the Pentagon, said John Pescatore, an information security analyst at Gartner Inc.

"This is a major concern, but not just when it goes offshore," Pescatore said. He called the focus on offshore antivirus developers "xenophobia," warning that U.S. antivirus software developers often hire programmers from Russia, China, and other countries. He said the concerns raised by the DoD should serve as a useful wake-up call for all organizations that buy antivirus software.

SERVICES

E-mails

RSS

Podcasts

CNNtoGO

CNN Pipeline

SEARCH

WEB CNN.COM

powered by

YAHOO! SEARCH

(Original *non*-parody version of this story published [here](#).)