Google complaint highlights China-based hacking

February 3 2010, By JOE McDONALD , AP Business Writer

(AP) -- Google's accusation that its e-mail accounts were hacked from China landed like a bombshell because it cast light on a problem that few companies will discuss: the pervasive threat from China-based cyberattacks.

The hacking that angered Google Inc. and hit dozens of other businesses adds to growing concern that China is a center for a global explosion of Internet crimes, part of a rash of attacks aimed at a wide array of targets, from a British military contractor to banks and chemical companies to a California software maker.

The government denies it is involved. But experts say the highly skilled attacks suggest the military, which is a leader in cyberwarfare research, or other government agencies might be breaking into computers to steal technology and trade secrets to help state companies.

"Chinese hacking activity is significant in quantity and quality," said Sami Saydjari, president of the consulting firm Cyber Defense Agency and a former U.S. National Security Agency official.

Officials in the United States, Germany and Britain say hackers linked to China's military have broken into government and defense systems. But attacks on commercial systems receive less attention because victims rarely come forward, possibly for fear it might erode trust in their businesses.

Google was the exception when it announced Jan. 12 that attacks hit it and at least 20 other companies. Google says it has "conclusive evidence" the attacks came from China but declined to say whether the government was involved.

Google cited the attacks and attempts to snoop on dissidents in announcing that it would stop censoring results on its China-based search engine and leave the country if the government does not loosen restrictions.

Only two other companies have disclosed they were targets in that attack - software maker Adobe Systems Inc. and Rackspace Inc., a Web hosting service.

Mikko Hypponen, chief research officer at Finnish security software maker F-Secure Corp., said his company has detected about two dozen attacks originating from China each month since 2005.

"There must be much more that go completely undetected," he said.

Hypponen said a large British military contractor with which his company worked discovered last year that information had leaked for 18 months from one of its computers to an Internet address in the Chinese territory of Hong Kong. He said similar attacks on military contractors were found in Germany, the Netherlands, Sweden and Finland.

Saydjari said other researchers have told him of dozens of U.S. companies that have been attacked from China but said he could not disclose their names or other details.

A key source of the skills required might be China's military. China's army supports hacker hobby clubs with as many as 100,000 members to develop a pool of possible recruits, according to Saydjari.

"China has a strategic goal of becoming the world-dominant economic power within this century. Certainly one way to do that faster is to steal industrial secrets," he said.

There are no estimates of losses attributable to hacking traced to China, but antivirus supplier McAfee Inc. says intellectual property worth an estimated $1 trillion was stolen worldwide through the Internet in 2008.

Separately, a Los Angeles law firm says it was hit Jan. 11 by an attack that appeared to originate in China after it filed a lawsuit for CyberSitter LLC, a software maker that accuses the Chinese government of stealing its code for use in a Web-filtering system.

The firm Gipson Hoffman & Pancione said e-mails sent to its lawyers contained malicious software designed to extract information from their computers.

Security firm Mandiant Corp. has dubbed such attacks - which allow repeated thefts over months or years - an "advanced persistent threat" and says each one it has studied over the past five years involved theft of information related to U.S.-China corporate acquisitions, negotiations or military acquisitions.

"The scale, operation and logistics of conducting these attacks - against the government, commercial and private sectors - indicates that they're state-sponsored," the company said in a report last month.

But even if an attack is traced to China, experts need to examine the computer used to be sure it was not hijacked by an attacker elsewhere. Consultants say security for many Chinese computers is so poor that they are vulnerable to being taken over and used to hide the source of attacks from elsewhere.

In the Google case, confirming the source would require China's cooperation, and Beijing has yet to respond to U.S. Secretary of State Hillary Rodham Clinton's appeal for an investigation.

"The 'smoking gun' proof is very hard to put together," said Graham Cluley, a researcher for Sophos, a British security software company.

China's Industry Ministry said in a statement that any suggestion the government is involved in any Internet attack "is groundless and aims to discredit China."

But China is no stranger to government-directed industrial espionage on a vast scale.

Intelligence experts say that since the 1970s, Beijing has carried on a quiet campaign to acquire foreign technology and other secrets by using Chinese businesspeople, students and scientists who travel abroad as part-time spies.

China, with the world's biggest population of Web users at more than 384 million, also has a history of hacking. In 1999, Web surfers defaced U.S. government sites after the mistaken American bombing of Beijing's Belgrade embassy killed three Chinese. Nationalists have attacked Web sites in Japan and Taiwan, the self-ruled island claimed by Beijing as its own territory.

More recent cases have shifted from vandalism to theft of government or trade secrets.

Last March, a Canadian group, the Information Warfare Monitor, said it found a China-based ring stole sensitive information from thousands of computers worldwide. Targets included the communications network of The Associated Press.

The government did not respond to the report's details but said it opposes computer crime and criticized the researchers for suggesting otherwise.

China has also ordered vendors that sell computer security technology to government agencies to reveal how it works under rules that take effect on May 1. Foreign companies operating there worry that might compromise systems used by banks and others to protect customer information and trade secrets.

Beijing is also pressing foreign financial firms to move more of their computer servers into China. That might require a switch to Chinese-made equipment with weaker protections.

Companies' reluctance to talk about China-based hacking "makes it difficult to make the case for action broadly," Saydjari said. "That might be why Google is parting from that history and sounding the alarm."