

Salesman: Hackers use Chinese company's servers

February 11 2011, By JOE McDONALD , AP Business Writer



In this file photo taken on Friday, March 12, 2010, people use computers at an Internet cafe in Fuyang, in central China's Anhui province. China has the world's biggest population of Internet users, with more than 450 million people online, and the government promotes Web use for business and education. But experts say security for many computers in China is so poor that they are vulnerable to being taken over and used to hide the source of attacks from elsewhere. (AP Photo) CHINA OUT

(AP) -- A Chinese man cited by a U.S. security firm as being linked to [cyberspying on Western oil companies](#) said Friday his company rents server space to hundreds of hackers.

The disclosure highlighted the pervasiveness of both professional and amateur hacking in China, a leading source of Internet crime. But it also left open the possibility that the hackers cited in a report Thursday by

McAfee Inc. might be non-Chinese who concealed their identities by routing thefts through computers in China.

The man cited by McAfee, Song Zhiyue, is a salesman for a company in the eastern city of Heze that rents server space. He said he has heard of Chinese hackers targeting U.S. [oil companies](#) but he declined to comment on McAfee's report. It said Song provided crucial infrastructure to the hackers but wasn't believed to be the mastermind.

"Our company alone has a great number of hackers" as customers, Song said in a telephone interview. "I have several hundred of them among all my customers."

Song said hackers using his company's services had an estimated 10,000 "meat computers" controlled remotely without the owners' knowledge. He said "yes" when asked whether such activities might be improper but he said Chinese authorities never have contacted him about them. He hung up the phone when a reporter asked for other details.

McAfee said the hackers broke into computers of oil and gas companies in the United States, Taiwan, Greece and Kazakhstan and stole sensitive information about bidding on oil and gas fields, operations and financing.

McAfee's report gave no indication that China's state-owned [oil companies](#) benefited from the spying. But Chinese energy companies are expanding abroad and such information could be useful as they compete for access to oil and gas resources.

Spokesmen for several American, British and Greek oil companies said they either were unaware of the hacking or could not comment on security matters.

A vice president of Taiwan's biggest oil company, Chinese Petroleum Corp., said it had detected no hacking of its computers. The executive, Paul Chen, said it would investigate.

China's police ministry did not immediately respond Friday to questions about whether it knew of the attacks or was investigating them. Taiwan's computer crime office was not aware of the attacks, said a police official. He spoke on condition of anonymity because he was not permitted to talk to reporters.

Security experts say China is a center for [Internet crime](#), including espionage against major companies. The government denies it is involved but experts say the high skill level of some attacks suggests the Chinese military, a leader in cyberwarfare research, or other agencies might be stealing technology and trade secrets to help state companies.

McAfee said the attacks in its report began in November 2009. It said extraction of information occurred from 9 a.m. to 5 p.m. Beijing time on weekdays, suggesting those involved were working a regular job, not freelancers or amateurs. It said they used hacking tools of Chinese origin that are prevalent on Chinese underground hacking forums.

The hackers expressed a strong interest in financial information, according to Dmitri Alperovitch, McAfee's vice president of threat research.

Thousands of Chinese computer enthusiasts belong to hacker clubs and experts say some are supported by China's military to develop a pool of possible recruits. Experts say military-trained civilian hackers also might work as contractors for companies that want to steal technology or business secrets from rivals.

China has the world's biggest population of Internet users, with more

than 450 million people online, and the government promotes Web use for business and education. But experts say security for many computers in China is so poor that they are vulnerable to being taken over and used to hide the source of attacks from elsewhere.

Last year, Google Inc. closed its China-based search engine after complaining of cyberattacks from China against its e-mail service.

That case highlighted the difficulty of tracking [hackers](#). Experts said that even if the Google attacks were traced to a computer in China, it would have to be examined in person to be sure it wasn't hijacked by an attacker abroad. Beijing has yet to respond publicly to U.S. Secretary of State Hillary Rodham Clinton's appeal last year for an investigation of the Google attacks.

More information: McAfee Inc.'s report: <http://bit.ly/hvV38n>

©2010 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: Salesman: Hackers use Chinese company's servers (2011, February 11) retrieved 26 April 2024 from <https://phys.org/news/2011-02-salesman-hackers-chinese-company-servers.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--