U.S. Security Firm Alleges Massive Chinese Hacking

CHRISTOPHER BODEEN, Associated Press

BEIJING (AP) — Cyberattacks that stole massive amounts of information from military contractors, energy companies and other key industries in the U.S. and elsewhere have been traced to the doorstep of a Chinese military unit, a U.S. security firm alleged Tuesday.

China's Foreign Ministry dismissed the report as "groundless," and the Defense Ministry denied any involvement in hacking attacks.

China has frequently been accused of hacking, but the report by Virginia-based Mandiant Corp. contains some of the most extensive and detailed accusations to date linking its military to a wave of cyberspying against U.S. and other foreign companies and government agencies.

Mandiant said it traced the hacking back to a neighborhood in the outskirts of Shanghai that includes a drab, white 12-story office building run by "Unit 61398" of the People's Liberation Army.

The unit "has systematically stolen hundreds of terabytes of data from at least 141 organizations," Mandiant wrote. By comparison, the U.S. Library of Congress 2006-2010 Twitter archive of about 170 billion tweets totals 133.2 terabytes.

"From our observations, it is one of the most prolific cyberespionage groups in terms of the sheer quantity of information stolen," the company said. It added that the unit has been in operation since at least 2006.

Mandiant said it decided that revealing the results of its investigation was worth the risk of the hackers changing their tactics and becoming even more difficult to trace.

"It is time to acknowledge the threat is originating in China, and we wanted to do our part to arm and prepare security professionals to combat that threat effectively," it said.

In a statement faxed to The Associated Press, the Defense Ministry firmly rejected any involvement in hacking, saying Chinese law forbids all activities harming Internet security.

"The Chinese government has always firmly combated such activities and the Chinese military has never supported any form of hacking activity," the ministry said. "Statements to the effect that the Chinese military takes part in Internet attacks are unprofessional and are not in accordance with the facts."

Chinese Foreign Ministry spokesman Hong Lei did not directly address the claims, but when questioned on the report Tuesday, he said he doubted the evidence would withstand scrutiny.

"To make groundless accusations based on some rough material is neither responsible nor professional," Hong told reporters at a regularly scheduled news conference.

Reiterating a standard China government response on hacking claims, Hong said China itself is a major victim of such crimes, including attacks originating in the United States.

"As of now, the cyberattacks and cybercrimes China has suffered are rising rapidly every year," Hong said.

Mandiant's methodology used in the investigation was sound, said Massimo Cotrozzi, managing director of KCS Group, a London-based international cyber investigation consulting firm that was not involved in Mandiant's research.

"No one as yet has provided the world conclusive evidence of a link between the Chinese military and the attacks. This report is the nearest thing to conclusive evidence that I have seen," Cotrozzi said.

Mandiant said its findings led it to alter the conclusion of a 2010 report it wrote on Chinese hacking, in which it said it was not possible to determine the extent of

government knowledge of such activities.

"The details we have analyzed during hundreds of investigations convince us that the groups conducting these activities are based primarily in China and that the Chinese government is aware of them," the company said in a summary of its latest report.

It said the hacking was traced to the 2nd Bureau of the People's Liberation Army General Staff's 3rd Department, most commonly known as unit 61398, in the Shanghai suburbs.

News of the report spread Tuesday on the Chinese Internet, with many commentators calling it an excuse for the U.S. to impose greater restrictions to contain China's growing technological prowess.

Graham Cluley, a British cybersecurity expert who was not involved in Mandiant's research, said people in the computer industry believe China's government is behind such attacks but have been unable to confirm the source.

"None of us would be very surprised or be uncomfortable saying we strongly suspect the Chinese authorities are involved in spying this way," said Cluley, a senior technology consultant for security firm Sophos in Britain.

"I think we are seeing a steady escalation" of sophistication in hacking, Cluley said. "This is really the new era of cybercrime. We've moved from kids in their bedroom and financially motivated crime to state-sponsored cybercrime, which is interested in stealing secrets and getting military or commercial advantage."

—

Associated Press writers Gillian Wong and Joe McDonald contributed to this report.