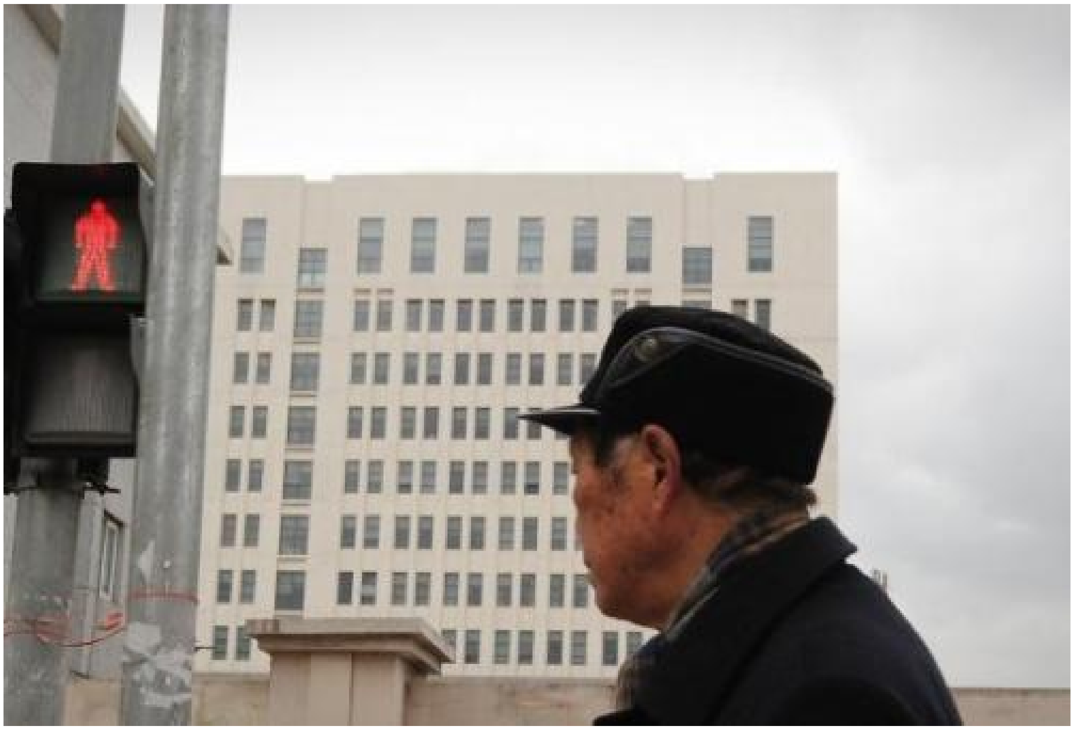
PHYS ORG

China: 'leading bad actor in cyberspace,' experts say

February 22 2013, by Carol Huang



A pedestrian is seen walking past a 12-storey building alleged in a report on February 19, 2013, by the Internet security firm Mandiant, as the home of a Chinese military-led hacking group after the firm reportedly traced a host of cyberattacks to the building in Shanghai's northern suburb of Gaoqiao.

China's full-throated denials of hacking and counter-accusations of its own do nothing to allay growing concern over large-scale cyberspying alleged in a bombshell report this week, Western analysts said.

Chinese officials and state-run media have lashed out after a report by a US firm laid out in unprecedented detail what Western officials and experts have long claimed: that China's army runs an aggressive hacking operation targeting US firms.

But James Lewis, a senior fellow based in Washington with the Center for Strategic and International Studies (CSIS), said: "No country breaks into tears and confesses when accused of espionage, so the denials can be dismissed.

"Many countries besides the US have concluded that China is the leading bad actor in cyberspace and China's espionage is on track to become a major international problem," he added.

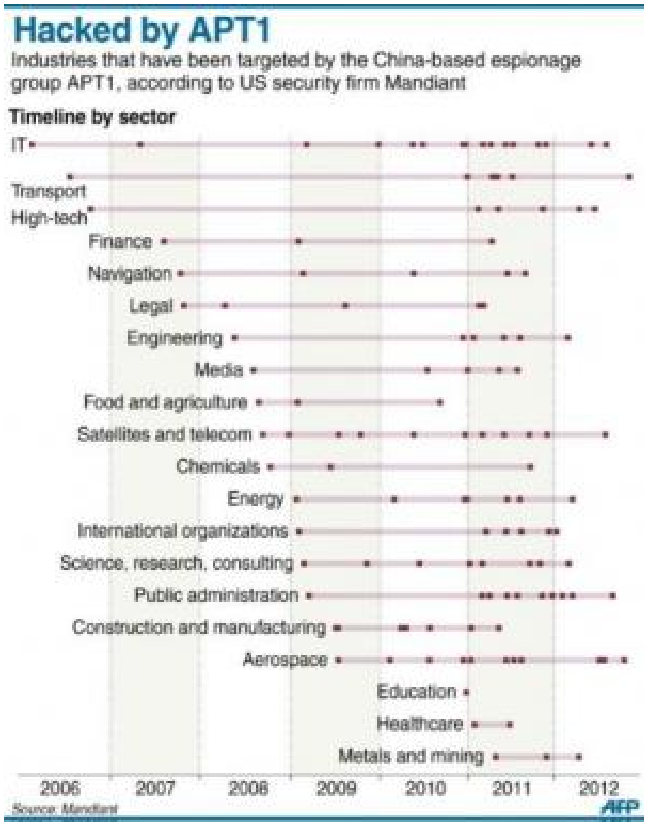
"Saying 'we're victims, too' won't deflect this."

The report from consultancy Mandiant alleged that hacking group "APT1" had stolen data from at least 141 organisations across 20 industries and was part of a Chinese military unit which investigators traced to an office block in Shanghai.

Although the account laid out the most detailed accusations yet of Chinese hacking, the rising power's online conduct had already drawn growing scrutiny.

Last month the New York Times and other American media outlets reported they had come under hacking attacks from China, and a US congressional report last year named the country as "the most threatening actor in cyberspace".

Beijing has rebuffed the allegations by countering that attacks tied to Chinese IP addresses do not necessarily originate from China, that their accusers have ulterior motives and that it too is a victim of hacking.



Graphic timeline of industries hacked by APT1, according to the Mandiant report.

Of about 10,000 attacks from overseas on Chinese websites last year, nearly three-quarters came from US IP addresses, the Xinhua state news agency said this month, citing the National Computer Network Emergency Response Coordination Centre.

Several Internet security firms with operations in China or Asia declined to comment on hacking attacks in light of the report.

But while Western powers have cyber-operations of their own, North American-based analysts said that Beijing's responses were disingenuous attempts to deflect attention from the mounting concern.

Major nations could be expected to carry out military and spy work in cyberspace as part of traditional war-planning and information-gathering, said Lewis, director of CSIS's technology and public policy programme.

Even so, China crossed a line by stealing commercial information, alarming Asian and Western countries, he added.

"The economic espionage part is probably the most troubling because it says something about China's willingness to play by the rules in the international system," he said.

Xinhua said in a commentary that Mandiant's report "reeks of a commercial stunt" and Washington has a "habit of accusing other nations based on phoney evidence".

Beijing's defence ministry also argued that there was no globally agreed definition of hacking while the foreign ministry touted an "international code of conduct" proposed in 2011 by China, Russia and others.

But Lewis dismissed the claim of a lack of consensus on defining Internet breaches, pointing to the Council of Europe Convention on Cybercrime along with documents at the United Nations and World Trade Organization.

Nearly 40 countries, not including China, have ratified the European document, which Lewis called the "global standard".

Sarah McKune, a senior researcher at the University of Toronto Munk School of Global Affairs, said the code of conduct that Beijing supported had stirred controversy for possibly limiting free expression and access to information.

China has probably suffered similar levels of hacking as other nations, she said. "All countries experience cybercrime and neither China nor the US are outliers in that respect."

But Beijing could more persuasively address the concerns by responding to the allegations rather than highlighting its role as a victim, she added.

The rhetoric from government bodies and state media "is frankly not the kind of response one would hope for from a major power committed to cooperation on cybersecurity," McKune said.

"Very specific assertions have been made in the Mandiant report that implicate actors based in China, and those assertions require a real response."

(c) 2013 AFP

Citation: China: 'leading bad actor in cyberspace,' experts say (2013, February 22) retrieved 2 May 2024 from https://phys.org/news/2013-02-china-bad-actor-cyberspace-experts.html