Chinese hackers targeting Australian law firms, an industry specialist warns

By Henry Belot

Published: 2017-11-30 · Archived: 2026-04-05 21:45:43 UTC

Chinese hackers are attacking Australian law firms that hold sensitive commercial information and have successfully hacked a research body, an industry specialist has warned.

Key points:

- Experts say threat of cyber espionage in the commercial world is high
- An Australian research and development body was targeted by Chinese hackers
- The origin of Chinese hackers remains unclear

The Chinese espionage group known as the Codoso team or APT-19 has been causing havoc internationally but is turning its attention to Australia.

The Australian Crime Commission's former cyber security manager, Tim Wellsmore, said any information obtained would likely be passed to Chinese companies.

Law firms hold confidential information that could give the companies inside knowledge ahead of business negotiations, mergers and acquisitions.

In some cases, these firms are seen as weak links as they have not taken cyber security as seriously as some of their clients.

Mr Wellsmore, who is now Director of Asia/Pacific Threat Intelligence for private security firm FireEye, said APT-19's origins remained unclear.

"Sometimes it is tricky to understand whether they are sitting there in uniforms working directly for the Chinese Government, or if they are sponsored and given resources but operate outside the Government hierarchy," he told the ABC.

> "APT-19 is certainly acting in support of Chinese state interests but at this stage we have not been able to attribute them to serving members of the Chinese Government."

FireEye observed at least seven phishing attacks directed at global law firms during May and June, some of which exploited vulnerabilities in Microsoft software.

A spokesman for the Department of the Prime Minister and Cabinet, which leads the Government's response to cybercrime, said hackers knew there was a low risk of being identified.

"[We] advise organisations to always think about the value of their data, know who has access to their data, know where their data is stored and review the protections in place to best secure their data," the spokesman said.

The department did not respond to questions about whether APT-19 had compromised any sensitive information.

Australian research body also hacked

Mr Wellsmore said his company had confirmed a Chinese attack on an Australian research and development body, but he would not say which one.

Tim Wellsmore would not say which Australian research and development body had been hacked. *(Twitter: Tim Wellsmore)*

"We have been involved in attacks in 2017 by the Chinese on research bodies within Australia and we continue to think this will be a focus for the Chinese in years to come," he said.

"There is a lot of research that would put them at a strategic advantage."

The Australian Cyber Security Centre report found espionage activity was likely to focus on a country's gaps in technology or know-how.

Fergus Hanson, head of cyber policy at the Australian Strategic Policy Institute, said disclosing Chinese attacks may encourage criminals to improve their methods.

"In terms of sectors being targeted, I don't have a bird's-eye view, but I'd assume anything that lined up with China's interests — mining, energy defence or companies that would lead to them, such as law firms and suppliers," Mr Hanson said.

APT-19 has 'global reach'

Greg Austin, a professor at the Australian Centre for Cyber Security at UNSW, said he was not surprised the group was targeting Australian companies.

"APT-19 has a global reach and its targeting may well be 'automated' so it would not be targeting Australian firms uniquely," he said.

"In such cases, it is inevitable that some Australian firms get caught up.

> "The threat of cyber espionage in the commercial world globally is very high because most firms present easy targets."

Professor Austin said many Chinese cyber criminals were not connected to the Chinese Government.

"Statistics on Chinese arrests of cyber criminals are staggering — tens of thousands of arrests each year, and hundreds of criminal gangs using cyber attack," he told the ABC.

"It is the only country with such a high number of reported arrests for cyber crime."
