Australia sounds warning over state-backed Chinese hackers

AFP- Australia's cyber intelligence agency sounded a rare warning Tuesday about the rising threat of state-backed Chinese hackers, saying they were "actively" looking for targets to compromise.

The Australian Signals Directorate singled out the APT40 hacking group in a detailed, technical advisory note that unpicked its evolving tradecraft.

"APT40 has repeatedly targeted Australian networks as well as government and private sector networks in the region, and the threat they pose to our networks is ongoing," the note read.

The Australian Signals Directorate said APT40 – meaning Advanced Persistent Threat – conducted "malicious cyber operations" for an arm of China's Ministry of State Security based in Hainan Province.

The directorate said APT40 looked to infiltrate old and forgotten devices that were still connected to sensitive computer networks.

Using these computers to gain an undetected "foothold", they were then able to "rapidly" exploit vulnerabilities and plunder information.

"APT40 is actively conducting regular reconnaissance against networks of interest in Australia, looking for opportunities to compromise its targets," the Australian Signals Directorate said.

Attribution of sophisticated cyberattacks is both technically difficult and politically fraught – and comes at the risk of angering China.

“In our current strategic circumstances, these attributions are increasingly important tools in deterring malicious cyber activity,” said Australian Defence Minister Richard Marles.

The advisory note was co-authored with input from the United States, the UK, Germany, Japan, South Korea and other international partners.

Cybersecurity experts have said inadequate safeguards and the stockpiling of sensitive customer information have made Australia a target for hackers.

Major ports handling 40 percent of Australia’s freight trade ground to a halt earlier this year after hackers infiltrated computers belonging to operator DP World.

Russia-based hackers in 2022 breached one of Australia’s largest private health insurers, accessing the data of more than nine million current and former customers.

In September 2022, telecom company Optus fell prey to a data breach of similar magnitude in which the personal details of up to 9.8 million people were accessed.

New Zealand’s government earlier this year blamed APT40 for a 2021 cyber attack that infiltrated its parliamentary computer network.

AFP