

Cyber Operations Tracker

Archived: 2026-04-05 17:31:07 UTC

Affiliations

- Also known as Earth Longzhi.

This threat actor has, since 2014, conducted operations backed by the Chinese government, including targeting the health-care and high-tech sectors and conducting espionage against political dissidents. It has simultaneously conducted its own for-profit illicit activity in the video games industry, amassing millions of dollars in digital currency to be sold to gamers on the black market. The threat actor operates outside of state control but is linked to other Chinese APT malware actors and tools on a part-time or contractual basis, or is a full-time, state-sponsored APT actor that simultaneously conducts nonstate campaigns for supplemental income. This threat actor is a notable example of the blurring lines between state-sponsored and commercial cyber criminals.

- United States, France, Japan, Singapore, United Kingdom, Hong Kong

Suspected state sponsor

- China

Type of incident

- Espionage

Target category

- Government
- Private sector

[Read more](#)

- [Double DragonAPT41, a dual espionage andcyber crime operationAPT41](#)

- [Chinese hacker group that works for both Beijing and personal gain identified](#)

Source: <https://www.cfr.org/cyber-operations/apt-41>