

# APT41 (Double Dragon): A Dual Espionage and Cyber Crime Operation

---

 [mandiant.com/resources/report-apt41-double-dragon-a-dual-espionage-and-cyber-crime-operation](https://www.mandiant.com/resources/report-apt41-double-dragon-a-dual-espionage-and-cyber-crime-operation)



## Breadcrumb

---

This comprehensive report details APT41, a prolific Chinese cyber threat group that carries out state-sponsored espionage activity in parallel with financially motivated operations. APT41 is unique among tracked China-based actors in that it leverages non-public malware typically reserved for espionage campaigns in what appears to be activity for personal gain. Explicit financially-motivated targeting is unusual among Chinese state-sponsored threat groups, and evidence suggests APT41 has conducted simultaneous cyber crime and cyber espionage operations from 2014 onward.

View the report to learn about:

- Historical and ongoing activity attributed to APT41

- The evolution of the group's tactics, techniques, and procedures (TTPs),
- Information on the individual actors and their malware toolset
- How these identifiers overlap with other known Chinese espionage operators

**[Download Now](#)**