

Forum:[Hack Forums](#)

Thread: [Anthropic Says Chinese AI Firms Used 16 Million Claude Queries to Copy Model](#)

Stanley - March 4, 2026, 8:20 am

Anthropic Says Chinese AI Firms Used 16 Million Claude Queries to Copy Model

Anthropic on Monday said it identified "industrial-scale campaigns" mounted by three artificial intelligence (AI) companies, DeepSeek, Moonshot AI, and MiniMax, to illegally extract Claude's capabilities to improve their own models.

The distillation attacks generated over 16 million exchanges with its large language model (LLM) through about 24,000 fraudulent accounts in violation of its terms

<https://thehackernews.com/2026/02/anthropic-says-chinese-ai-firms-used-16.html>

Immortal - March 4, 2026, 2:50 pm

The scale here is impressive, but the method is old school brute force. What Anthropic is calling "industrial-scale intellectual property theft" is just high-volume model distillation. If you have an API and a budget, you have a dataset.

The interesting part isn't that DeepSeek or MiniMax used 24,000 "fraudulent" accounts—that's just basic sybil management. The real takeaway is the "hydra cluster" proxy architecture they used to bypass rate limits and geographical blocks. Routing 16 million exchanges through commercial proxies without tripping a sub-network ban for months shows they have a very refined understanding of Anthropic's detection heuristics.

Also, let's be real: every major LLM lab is doing some form of this to their competitors. The only reason Anthropic is making a public stink about it now is to lobby for tighter export controls and "national security" protections. It's a PR move to mask the fact that their API was effectively a subsidized training gym for the East for the last six months.

If anyone has a dump of the prompts used by the MiniMax cluster, PM me. I'm curious to see their "agentic reasoning" extraction templates.