# ARTEX: A Free AI Tool That Runs Hacking Tests on Its Own, With Control Panels Left Open Online

Kabui, Charles

2026-11-10

Read at ToKnow.ai




ARTEX is a free Chinese AI tool, released in July, that runs security tests on its own. Security teams use such tests, called penetration testing, to find weak spots in their own systems. A user types a goal, such as getting into an administrator page. A planner agent splits the goal

into steps, like a manager handing out jobs, and worker agents run scanning tools and report back until the goal is met. A web control panel shows the progress. Censys, a company that scans the internet and records what each server shows, counted 1,465 addresses showing an ARTEX control panel in early November. About 815 look distinct once identical setups are set aside. Check Point, counting separately, found 1,608 live panels.

TechCrunch reports the panels open without a password, so anyone who finds one can use it. Censys says some likely belong to authorized testers. CrowdStrike linked one ARTEX server to a campaign that stole data from South Korean financial organizations between late September and early October. That operator had left public folders holding AI chat logs and settings files, and Censys found 32 more open folders on other ARTEX systems, holding attack tools. Check Point read the chat records of another operator, who ran two consoles for two weeks to steal software signing certificates and mostly asked the agents for progress. It estimates the AI fees at $700 to $1,500. The developer stopped public releases on October 8 and the GitHub page is gone, but copies still circulate.

Read More: Anthropic's red team on GLM-5.3, an open-weight model that builds working cyber exploits, one of the models CrowdStrike lists in the South Korean case

Sources:

- ARTEX: Agentic Asbestos (Censys)
- Unknown Threat Actor Uses AI-Driven ARTEX to Target South Korean Finance (CrowdStrike)
- Hacking on Autopilot: Inside ARTEX Cybercrime Campaigns (Check Point Research)
- Hundreds of Artex AI hacking tools found publicly exposed to the web (TechCrunch)

---

***Disclaimer:*** *For information only. Accuracy or completeness not guaranteed. Illegal use prohibited. Not professional advice or solicitation.* ***Read more:*** */terms-of-service*