

Chinese-speaking hacker used AI agents to break into sites of 100+ companies for about US\$5000

Source copy kept by wheresthe.ai for the story "Chinese-speaking hacker used AI agents to break into sites of 100+ companies for about US\$5000" (<https://wheresthe.ai/d/us-chinese-speaking-hacker-used-ai-agents-to-break-into-site-2026-10/>).

Source: <https://www.itnews.com.au/news/how-one-hacker-used-ai-agents-and-a-few-thousand-dollars-to-break-into-scores-of-sites-629764>

Text saved 20 Oct 2026 (the page as published).

SHA-256 of the saved text: 76e401bafefc5f16f39eae6c315f9d4fedf1b19fb54d938e4ccde1ace38f136f

[Home](#)

[News](#)

[Technology](#)

[Security](#)

How one hacker used AI agents and a few thousand dollars to break into scores of sites

By

Raphael Satter

Oct 20 2026 1:42PM

Ecommerce sites in Australia, Canada, US and Japan targeted.

Over the past couple of weeks, a cyber security researcher watched as a Chinese-speaking hacker broke into websites belonging to more than 100 companies, including farm equipment maker Deere, home appliance company SharkNinja and engine manufacturer Cummins.

Yet the hacker did almost none of the work.

The cybercriminal instead outsourced the hacking spree almost entirely to artificial intelligence, tasking AI agents with spending hours autonomously probing and breaking into targeted sites, according to Snorre Fagerland, principal threat researcher at the cyber security company NorForge.

In a report , Fagerland said the hacker was one of several he discovered while scanning the web for inadvertently exposed instances of Cairn, an open-source AI problem-solving platform popular with hackers.

Beginning around October 2, Fagerland said he found about two dozen instances of Cairn being used for malicious activity, which allowed him to quietly peer over the cybercriminals' shoulders as they set their AI tools loose on the world.

Fagerland's report on the Chinese-speaking hacker did not name the victims, but Reuters was able to establish the victims' identities by independently reviewing the hacker's Cairn activity.

At a time of rising anxiety over the power of autonomous AI tools, Fagerland said his find was real-life evidence that commercially available AI agents could pull off complex intrusions from start to finish without human intervention, a dramatic boost to the power of a single malicious actor.

"It's a new world now," said Fagerland.

Reuters could not ascertain the degree to which the breaches resulted in unauthorised extraction of data.

Deere told Reuters it had taken "necessary remediation actions" following the incident and had "no indication that sensitive information was accessed."

SharkNinja said the hack had hit a standalone site carrying only product support information and that the threat had been contained.

Cummins said it was "investigating the report of a potential cyber-attack on a website operated by one of our third-

party vendors."

Two smaller businesses also acknowledged being compromised.

Other victims listed in the Cairn data did not return messages.

Few instructions, many hacks

One of the hackers that Fagerland observed stole a trove of credit card data.

Another tried to get AI agents to rob a cryptocurrency exchange.

The Chinese-speaking hacker was the most prolific.

Beginning on September 25, they set their AI army loose against US, Canadian, Australian and Japanese ecommerce websites.

Their instructions were terse, sketching out their preferred intrusion tactics in fewer than 100 Chinese characters.

As of late last week, their agents had attempted to break into more than 1200 sites.

Successful intrusions typically took around 23 hours of poking and prodding for vulnerabilities.

Fagerland estimated that the campaign, which appeared to be using a mixture of China's DeepSeek and Anthropic's Claude Code, had chewed up roughly US\$5000 (\$7162) worth of tokens, or about US\$50 per successful hack.

Fagerland — who has worked in cyber security for nearly three decades — said he was impressed by some of the techniques the agents used to compromise their victims.

In one case, after failing to find any weaknesses in a big company's public-facing application, the AI agents pored through digital records to find associated infrastructure, located a public-facing control panel, discovered a subtle weakness in the way it processed data, and after hours of trial and error, reported leveraging it to trick the server into executing malicious commands.

"It's not straightforward to come up with solutions like that," Fagerland said.

"It's not script kiddie stuff," he added.

Cairn's author, whose social media handle is "le1xia0", acknowledged receipt of a Reuters message but did not immediately answer a list of questions.

In a recent post on X, they said their platform was "an innovative type of multi-agent architecture and was not designed for hacking attacks.

"If it is used to carry out harmful hacking attacks, that is not my intention."

No supervision needed

The ability of agentic AI systems to autonomously discover vulnerabilities, conduct intrusions, and steal data is a source of increasing anxiety around the world.

Rogue agents inadvertently unleashed by major AI companies have hacked their way out of computer labs, broken into government websites, and engaged in unsanctioned social engineering attempts.

South Korea and Japan have in recent weeks been buffeted by a series of well-publicised hacks attributed to AI-using cybercriminals.

AI agents are increasingly becoming staples of the cybercriminal underground.

In August, the Israeli firm Gambit Security found that Russian-speaking extortionists had leveraged SpaceX's Cursor AI tool to break into seven organisations.

In September, Gambit documented an AI agent-driven spree that resulted in breaches at 25 companies and the theft of at least 600,000 credit card records.

Last week, the cyber intelligence company BitSight said that discussions about how to use autonomous agents were surging across cybercriminal forums.

Fagerland said he had previously assumed hacker-agents would need at least some supervision.

He said it was now obvious that the technology had moved past that.

"The development in this field is astounding," he said.

Add iTnews as your trusted source

Got a news tip for our journalists? Share it with us anonymously here .

© 2019 Thomson Reuters. [Click for Restrictions](#).

Tags:

[ai](#) [artificial intelligence](#) [cairn](#) [norforge](#) [security](#)

Partner Content

[Learn more](#) → ">Partner Content

Who owns your brand's AI reputation?

[Learn more](#) → ">Promoted Content

From ambition to impact: The next era of government transformation.

[Learn more](#) → ">Promoted Content

How David Jones, Canva and others are putting agentic AI to work

iTnews State of Security Breakfast comes to Sydney

SPONSORED RESOURCES

[Craft your ideal hybrid multicloud strategy](#)

[Secure your AI future with generative AI defense](#)

[See how F5 protects modern applications against evolving threats](#)

[8 Benefits of a Backup Service for IaaS, PaaS, and SaaS](#)

[5 Essentials for Effortless SaaS Data Resilience](#)

Events

[RIMPA Live Convention 2026](#)

[What's Next?](#)

[iTnews Benchmark Security Awards 2026](#)

[iTnews State of Security Breakfast Sydney](#)

[iTnews Executive Retreat - Security Leaders Edition - VIC](#)