AI server attacked by hackers

AI server attacked by hackers

Over two and a half months, a group of hackers used both Claude Code and ChatGPT to steal private information from the Mexican government.

A new paper warns AI systems can now hack vulnerable servers and act autonomously, raising fresh questions about risk, control and containment.

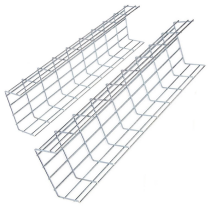
Cybersecurity researchers have recently uncovered a significant breach involving hundreds of AI compute servers. Hackers exploited an open-source software called Ray, which is ...

A community-driven database of AI-related security incidents, data breaches, and leaks. Track and discover the latest AI security vulnerabilities.

AI-enabled attacks rose 89% this year. Explore 9 verified incidents from 2026, including autonomous breaches and data leaks, and learn how to protect your organization.

The researchers found a malware operation that''s been hijacking AI servers to mine cryptocurrency and steal sensitive credentials. The detected infections started by the end of 2024 ...

Security researchers have documented a surge in coordinated attacks targeting artificial intelligence infrastructure, with more than 91,000 malicious sessions recorded between October 2025 ...



Security researchers have identified over 91,000 attack sessions targeting AI infrastructure between October 2025 and January 2026, exposing systematic campaigns against large language ...

An AI agent just autonomously exploited a FreeBSD kernel vulnerability in four hours, signaling a fundamental shift in the economics of offensive cyber capability.

A new investigation by GreyNoise reveals a massive wave of over 90,000 attacks targeting AI tools like Ollama and OpenAI. Experts warn that hackers are conducting ...

Contact Us

For more information, pricing, or custom network solutions, please contact us:

Website: https://www.hashherbcafe.co.za
Email: hello@hashherbcafe.co.za
Phone: +27 63 814 7295
Address: 15 Galaxy Road, Linbro Business Park, Johannesburg, 2065, South Africa

This document is for informational purposes only. Specifications subject to change without notice.