# Fake Web3 accelerator uses malicious npm packages to deliver stealers and backdoors



A fake Web3 accelerator has been spreading information stealers and backdoors to Windows and macOS systems through malicious npm packages, offering free AI credits, coding tools and security audits as bait.

- The campaign targets both Windows and macOS machines.
- Malicious npm packages deliver information stealers and backdoors.
- The lure is free AI credits for Anthropic Claude and Google Gemini, coding tools and security audits.
- The findings were attributed to Elastic; the headline also refers to hijacking of AI agent traffic.

## What was reported

According to The Hacker News, a fake Web3 accelerator has been distributing information-stealing malware and backdoors to Windows and macOS systems. The delivery route is malicious npm packages, and the pretext is an offer of free artificial intelligence credits for Anthropic Claude and Google Gemini, along with coding tools and security audits.

The report quotes Elastic as stating that the tools delivered information stealers and backdoors for both macOS and Windows machines. The headline also mentions hijacking of AI agent traffic, but the excerpt available to us does not explain how this works.

## Why it matters

The lure targets developers and technical teams who are likely to install packages and trial AI tooling quickly. A stealer or backdoor on a developer workstation can expose credentials and give an attacker a foothold, so the risk extends beyond the individual device. Free credits and free audits are an attractive offer, which is why such approaches deserve scrutiny.

The source excerpt does not name the packages, the accelerator, the number of victims or the attribution, so we do not speculate on them.

## What to do next

Treat unsolicited offers of free AI credits, tools or audits as untrusted until verified, and review how developers obtain and install npm dependencies. The actions below are practical starting points.

## What to do now

1. Warn developers and engineering teams about unsolicited offers of free AI credits, tools or security audits, and require verification before engaging.
2. Restrict npm installs to approved registries or an internal mirror, and review newly added dependencies before use.
3. Run developer tooling on managed endpoints with EDR coverage on both Windows and macOS.
4. Search endpoints and build systems for recently installed unfamiliar npm packages, and rotate credentials on any device where one is found.
5. Review how AI tools and agents are configured and which API keys they use, and keep keys scoped and revocable.