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



A fake Web3 accelerator offering free AI credits, coding tools and security audits is delivering information stealers and backdoors to Windows and macOS machines through malicious npm packages, according to Elastic.

- The lure is a fake Web3 accelerator promising free AI credits for Anthropic Claude and Google Gemini, plus coding tools and security audits.
- Malicious npm packages deliver the payloads.
- Both Windows and macOS systems are targeted.
- Elastic reports the tools delivered information-stealing malware and backdoors.
- The headline also refers to hijacking of AI agent traffic; the excerpt we reviewed gives no further detail on this.

A fake Web3 accelerator has been seen distributing malware to developers' machines using malicious npm packages. According to Elastic, the tools delivered information-stealing malware and backdoors for both macOS and Windows.

How the campaign works

The operators present themselves as an accelerator program. The offers are designed to appeal to developers and technical teams: free AI credits for Anthropic Claude and Google Gemini, coding tools, and security audits. The npm packages are the delivery mechanism for the malicious code.

The source headline also says the campaign hijacks AI agent traffic. The portion of the report available to us does not explain how, so organisations should avoid assuming specifics until the full technical analysis is reviewed.

Why it matters for regulated institutions

Information stealers typically target credentials and other data held on a workstation, and backdoors give an attacker continued access. Developer endpoints often hold access to source code, cloud services and internal systems, so a compromised developer machine can become an entry point to wider environments. Offers of free AI credits and audits are plausible to technical staff, which makes this a social-engineering risk as much as a technical one.

The practical response is to treat unsolicited packages and programs, however attractive, as untrusted until verified, and to check whether any such packages have already reached your environment.

What to do now

1. Search developer machines and build systems for recently installed npm packages from unfamiliar publishers or tied to accelerator or free-credit offers.
2. Require approval and review before new npm dependencies are added, and use an internal registry or allow-list where feasible.
3. Remind developers and technical staff not to engage with unsolicited offers of free AI credits, tools or security audits.
4. Ensure EDR coverage on Windows and macOS developer endpoints, and escalate any signs of stealer or backdoor activity.
5. If a suspect package was installed, isolate the device and rotate credentials and tokens it could access, including AI service keys.
6. Review the full Elastic analysis for indicators and add them to detection tooling.