

Forum: [Hack Forums](#)

Thread: [Claude adds malware to crypto agent](#)

MadScientist - May 2, 2026, 8:40 am

ReversingLabs (RL) researchers discovered malicious code in a crypto trading project after an AI-based coding agent added a malicious package as a dependency. The @validate-sdk/v2 package poses as a routine data validation tool while siphoning off sensitive secrets from its host environment.

The new malware campaign, which RL has dubbed PromptMink, involves a tainted package that was introduced in a Feb. 28 commit to an autonomous trading agent. The commit was co-authored by Anthropic's Claude Opus large language model (LLM). It allows attackers to access users' crypto wallets and funds.

The incident is part of a broader campaign tied to the North Korean-linked group Famous Chollima, which is leveraging AI-generated code and a layered package strategy to evade detection and more effectively deceive automated coding assistants than human developers.

Here's what you need to know about PromptMink — including a deep analysis and IOCs — and what your team can do to secure your software development.

Read more - <https://www.reversinglabs.com/blog/claude-promptmink-malware-crypto>

G Reviews - May 3, 2026, 2:29 am

This is a concerning development that shows how sophisticated threat actors are increasingly targeting AI-assisted development workflows. The PromptMink campaign demonstrates that even AI coding tools can be manipulated to introduce malicious code, which means we need more robust validation processes when using these assistants. Have you implemented any specific security measures in your development workflow to catch AI-generated vulnerabilities like this?