

Six npm Packages Use Ethereum Transactions to Retrieve Malicious Payloads

By Sonatype Research Team

Published: 2026-08-10 · Archived: 2026-08-14 02:01:42 UTC

TL;DR

- Sonatype Research Labs identified six npm packages delivering the same malicious payload: three hijacked legitimate packages and three additional malicious packages, tracked as [sonatype-2026-005899](#) and [sonatype-2026-005901](#).
- The malware uses the same Ethereum wallet address [identified by OpenSourceMalware](#) in activity attributed to the DPRK-linked Contagious Interview campaign, using the "NullReceiver" technique to locate infrastructure hosting additional JavaScript payloads.
- Organizations that installed the affected versions should remove them and investigate the impacted environment for follow-on payload execution or compromise.

On August 10, 2026, Sonatype Research Labs identified six npm packages containing the same malicious payload, including three compromised legitimate packages and three packages published with the malware already present.

The payload uses Ethereum blockchain transactions to locate infrastructure hosting additional JavaScript malware. Sonatype researchers confirmed the six packages use the same Ethereum wallet address in recent activity attributed to the DPRK-linked Contagious Interview campaign. OpenSourceMalware dubbed the specific blockchain-based command-and-control technique "NullReceiver," while Contagious Interview refers to the broader campaign associated with the Lazarus APT group.

Six npm Packages Deliver the Same Malware

According to Sonatype's Adam Reynolds, the affected packages fall into two groups.

Three are legitimate npm packages that appear to have been hijacked to publish malicious versions, which Sonatype is tracking as sonatype-2026-005899:

- @kolbo/mcp@1.57.1
- agentgui@1.0.1127
- godot-kit@1.0.1786316795

In the hijacked packages, the payload was embedded into a file that already existed in the legitimate package, pictured here in the last line of database.js in agentgui.

- envpack-conf@1.0.1
- postcss-initial-provider@3.0.4
- tailwindcss-motion-advanced@1.0.1

Despite the different paths into npm, all six packages contain the same malicious payload and are associated with the same wallet address.

The implementation Sonatype observed is also more extensive than the [NullReceiver](#) behavior. The loader can query several Ethereum RPC providers, race requests between them, use batched JSON-RPC calls, and fall back to the Blockscout API to locate the relevant transaction. This gives the malware multiple ways to recover its C2 infrastructure if one method fails.

Same Payload, Two Paths Into npm

The six packages show the same malware being distributed in two different ways: by compromising packages developers may already trust, and by publishing new packages created specifically to deliver the malicious payload.

In the three hijacked packages, substantial legitimate functionality remains intact, with the malicious loader appended to the end of a legitimate file, which is the same behavior we saw with the DPRK-linked [PolinRider campaign](#).

The independently published packages also contain legitimate-looking functionality: envpack-conf includes package-configuration code, postcss-initial-provider includes normal PostCSS plugin code, and tailwindcss-motion-advanced carries the loader inside utils.min.js.

A Familiar DPRK-Linked Technique

The six packages use a technique that closely resembles **NullReceiver**, a blockchain-based command-and-control method used in the DPRK-linked Contagious Interview campaign, recently spotted by [OpenSourceMalware](#) in two npm packages, bianira-ui and fluid-type-ui.

In that activity, the malware looked up an attacker-controlled Ethereum wallet, read the recipient address from its latest outbound transaction, decoded a C2 IP from that address, and then connected to it. OpenSourceMalware attributed those packages to the DPRK Contagious Interview campaign.

Sonatype Research Labs observed similar tradecraft here: hijacked packages, blockchain-based retrieval of follow-on infrastructure, and malicious code embedded into or shipped with package files.

Check Your Builds for These Six npm Packages

Developers and security teams should check their environments for the six affected npm packages and remove any impacted versions.

For the three hijacked packages, the risk is especially easy to miss because the malicious code arrived through packages developers may already recognize and trust. The three additional malicious packages show the same payload can also be introduced through newly published packages.

If any affected package was installed, teams should investigate for follow-on JavaScript execution and other signs of compromise.

[Sonatype Research Labs](#) is continuing to investigate related npm activity and will update its findings as additional packages or infrastructure are identified.

Tags

npm Open Source security research malicious code npm Malware Analysis Malware open source malware Sonatype Guide

Source: <https://www.sonatype.com/blog/six-npm-packages-use-ethereum-transactions-to-retrieve-malicious-payloads>