# Hacker Infects Node.js Package to Steal from Bitcoin Wallets

Archived: 2026-04-06 01:51:33 UTC

A Node.js module with nearly two million downloads a week was compromised after the library was injected with malicious code programmed to steal bitcoins in wallet apps.

The Node.js library is called “event-stream,” a toolkit for developers to create and work with streams. The malicious code in question was identified earlier this week to be added to the library’s version 3.3.6, published in September and has since been downloaded by millions of application programmers.

The event-stream module was originally by Dominic Tarr, who maintained the library before handing the reins to a project contributor who goes by the handle “right9ctrl.” Tarr indicated that he has not used the module for years and transferred its ownership after he received an email regarding its maintenance. The new maintainer has since released event-stream version 3.3.6, with a new dependency called “flatmap-stream” that contained the malicious code.

Since the flatmap-stream module was encrypted, the malicious code remained undetected for over two months until Ayrton Sparling (FallingSnow) flagged the issue on GitHub last week.

Open-source project manager and event-stream host Node Package Manager (NPM) has since reviewed the obfuscated code and encrypted payload. NPM found that the malicious module has been designed to swipe bitcoins from Copay wallets, a wallet app by Bitcoin payment platform BitPay. Copay is said to have incorporated event-stream into its app.

The malicious code attempted to steal bitcoins stored in the Copay wallets and distributed via NPM in order to reportedly transfer the funds to a server located in Kuala Lumpur.

The backdoor has since been removed from NPM on Monday this week. BitPay has also published an advisory that users should update their Copay wallets (versions 5.0.2 through 5.1.0) to version 5.2.0 as the older versions may have been compromised. The company also clarified that the BitPay app was not affected by the malicious code.

### Defending Against Cryptocurrency-Mining Malware

Copay users are advised to avoid running or opening affected versions (5.0.2 to 5.1.0) and immediately update their wallets to version 5.2.0. Users who ran the vulnerable versions of the software should assume that their private keys have been affected by the malware and should move their funds to Copay 5.2.0 or later.

This incident highlights how an attacker can stealthily infect systems with cryptocurrency mining-malware. The hacker here has gained access to a popular JavaScript library to steal coins in wallet apps. Aside from stolen funds, machines infected by cryptocurrency-mining malware can cause significant performance issues. Users can consider adopting security solutions that can defend against cryptocurrency-mining malware through a cross-generational blend of threat defense techniques. Trend Micro™ XGen™ security provides high-fidelity machine learning that can secure the gateway and endpoint, and protect physical, virtual, and cloud workloads. With technologies that employ web/URL filtering, behavioral analysis, and custom sandboxing, XGen security offers protection against ever-changing threats that bypass traditional controls and exploit known and unknown vulnerabilities. XGen security also powers Trend Micro's suite of security solutions: Hybrid Cloud Security, User Protection, and Network Defense.

Trend Micro™ Deep Discovery Inspector™ protects customers via this DDI rule:

- DDI Rule ID 26: C&C callback attempt

**Indicators of Compromise (IoCs)**

**Related hashes (SHA-256):**

- afc100fb28f7bac05e41d9ae33f184502b8068642b7fd05970eb72bf1786892c - Coinminer.Win32.MALBTC.AA
- 8b90859b19e3e3dea8d923996709210ed48ff3249563f56ff12eb1936ffcc295 - Coinminer.Win32.MALBTC.AA

HIDE

**Like it? Add this infographic to your site:**
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

---