Malicious npm and PyPI Packages Disguised as Dev Tools to Steal Credentials

By Mandvi

Published: 2025-04-22 · Archived: 2026-04-05 18:12:16 UTC

The Socket Threat Research Team has identified a new supply chain threat targeting developers in the crypto space: three malicious packages one on npm and two on PyPI masquerading as legitimate developer utilities while covertly exfiltrating sensitive wallet credentials.

These packages, “react-native-scrollpageviewtest” (npm), “web3x” (PyPI), and “herewalletbot” (PyPI), have collectively amassed nearly 8,000 downloads, exposing unsuspecting developers to significant asset loss by harvesting mnemonic seed phrases and private keys.

Open Source Registries Targeted by Credential-Harvesting Malware

The npm package “react-native-scrollpageviewtest,” first released in 2021, camouflages itself as a benign page-scrolling tool for React Native.

Instead, it employs advanced obfuscation by dynamically constructing sensitive API names in memory, splitting relevant strings to evade static detection, and encoding key controller references in Base64.

Once loaded, the package extracts mnemonic seed phrases and private keys from local wallet storage, prepends each exfiltrated secret with randomized data, and stealthily transmits them to a Google Analytics endpoint using standard event telemetry formats.

This abuse of Google Analytics (Tracking ID UA-215070146-1) leverages the routine whitelisting of analytics domains in enterprise environments, ensuring that the attacker’s exfiltration attempts blend in with normal network traffic and evade conventional perimeter defenses.

In parallel, two PyPI packages “web3x” and “herewalletbot” exploit the trust of Python developers with similar credential-stealing techniques.

“web3x” presents as an Ethereum wallet balance checker but, upon execution, immediately prompts the user for a mnemonic seed phrase and relays it, along with wallet balances, to an attacker-controlled Telegram bot via the Telegram Bot API.

The exfiltration is near-instantaneous and silent, enabling rapid wallet compromise.

Threat Actors Use Google Analytics and Telegram Bots for Exfiltration

The “herewalletbot” package, meanwhile, impersonates an automation tool for Telegram-based crypto rewards.

It scripts a headless browser session, guiding unsuspecting users through the Telegram login process and directly soliciting their mnemonic seed phrase under the guise of a rewards claim.

This seed phrase is then exfiltrated into the chat window of a Telegram bot (@herewalletbot), giving the attacker full control over the victim's crypto assets.

Despite apparent attempts by its author to conceal this functionality, including amending public documentation while retaining the malicious logic, the package continued to compromise credentials until publicly flagged.

The threat actors behind these campaigns demonstrate operational sophistication: leveraging social engineering, string obfuscation, staged payload exfiltration, and nuanced detection evasion.

Their techniques such as Base64-encrypted API references, randomized exfiltration payloads, hardcoded bot tokens, and conditional execution to avoid developer or test environments underscore a sharp focus on persistence and stealth.

The persistence of these packages on public registries underscores a critical risk: open-source ecosystems remain a high-value vector for supply chain compromise.

Developers who inadvertently install such modules risk catastrophic loss, particularly in the context of cryptocurrency, where stolen mnemonics and private keys enable irreversible asset transfers.

Security experts urge developers to remain vigilant: never enter or transmit seed phrases or private keys to any utility, script, or package.

Tools that request such credentials especially within automation, wallet management, or browser integration contexts should be treated with extreme suspicion.

Organizations should adopt proactive measures, including automated dependency scanning, runtime monitoring, and strict code review, especially for packages related to Web3, authentication, or browser automation.

According to the Report, Socket and similar platforms provide essential tooling to proactively analyze dependencies and block threats before code reaches production.

Developers are advised to utilize these resources and consistently apply the security principle of explicit trust, particularly when handling high-value credentials within open-source pipelines.

Indicators of Compromise (IOC)

Type	Indicator / Value	Description
Package	react-native-scrollpageviewtest	Malicious npm package
Package	web3x	Malicious PyPI package

Type	Indicator / Value	Description
Package	herewalletbot	Malicious PyPI package
Endpoint	@herewalletbot	Telegram bot for exfiltration
Endpoint	hxxps://web[.]telegram[.]org/k/#@herewalletbot	Telegram bot phishing URL
Token	5847347125:AAG-WskaS485OUlGLfa5AKEMW1aKYymplPQ	Telegram bot token (web3x)
Email	twoplusten@163[.]com	npm threat actor email (twoplus)
Email	xeallmail@mitico[.]org	PyPI threat actor email (tonymevbots)
Email	bevansatria@gmail[.]com	PyPI threat actor email (vannszs)
Alias	twoplus	npm threat actor alias
Alias	tonymevbots	PyPI threat actor alias
Alias	vannszs	PyPI/GitHub threat actor alias
GitHub	https://github.com/vannszs/HotWalletBot/	Related malicious repo (defunct)
Google Analytics	UA-215070146-1	Used for exfiltration by npm package

Find this Story Interesting! Follow us on LinkedIn and X to Get More Instant updates

Mandvi

Mandvi is a Security Reporter covering data breaches, malware, cyberattacks, data leaks, and more at Cyber Press.
