

xmrwallet.com — Technical Evidence Report

PhishDestroy Research — February 2026

Executive Summary

xmrwallet.com is a fraudulent Monero (XMR) web wallet service that has systematically stolen user funds since at least 2016. Through server-side transaction hijacking and private view key exfiltration, the service has defrauded **15+ documented victims** of an estimated **\$2,000,000+ USD** in Monero cryptocurrency. The operator, identified as **Nathalie Roy** (GitHub: nathroy), has engaged in active evidence destruction — deleting 21+ GitHub issues after public exposure — and has attempted to establish escape domains (xmrwallet.cc, xmrwallet.biz), both of which have since been suspended.

This report presents the complete technical evidence chain, from code-level analysis to victim documentation, establishing xmrwallet.com as a deliberate theft operation masquerading as a privacy-focused cryptocurrency wallet.

1. Private View Key Exfiltration

The session_key Mechanism

Upon wallet creation or login, xmrwallet.com generates a `session_key` parameter that is transmitted to the operator's server. Reverse engineering reveals this key is a **Base64-encoded concatenation** of the user's Monero address and private view key:

Component	Description
Format	Base64(address + viewkey)
Decoded structure	First 95 characters = Monero public address; Remaining 64 characters = Private view key
Transmission	Sent via HTTPS POST to xmrwallet.com backend on every session
Persistence	Stored server-side, enabling ongoing surveillance of victim wallets

With the private view key, the operator can:

- **Monitor all incoming transactions** to the victim's wallet in real time
- **Calculate the wallet's exact balance** at any point
- **Time theft transactions** to maximize the stolen amount
- **Confirm successful fund extraction** after sweeping

Why This Matters

Legitimate Monero web wallets (such as the official MyMonero) never transmit raw private view keys to the server in this manner. The `session_key` construction is a deliberate exfiltration mechanism with no legitimate purpose.

2. Server-Side Transaction Hijacking

The raw_tx_and_hash Analysis

When a user initiates a transaction on xmrwallet.com, the server returns a `raw_tx_and_hash` object. In legitimate transactions, the `raw` field contains the signed transaction hex. Analysis of stolen transactions reveals:

Field	Legitimate Value	Fraudulent Value
raw_tx_and_hash.raw	Full transaction hex (hundreds of characters)	∅ (zero)
raw_tx_and_hash.type	transfer	swept
raw_tx_and_hash.hash	Valid TX hash	Hash of operator's sweep transaction

When `raw = ∅` and `type = 'swept'`, the server has:

1. **Intercepted** the user's intended transaction
2. **Replaced it** with a sweep transaction sending all funds to the operator's wallet
3. **Returned a fake confirmation** to the user's browser
4. The user sees a "successful" transaction while their entire balance is stolen

Technical Flow

User submits TX → Server receives request → Server ignores user's destination
 → Server constructs sweep TX to operator wallet → Server signs with stolen keys
 → raw_tx_and_hash.raw = ∅, type = 'swept' returned → User sees fake confirmation
 → Funds arrive in operator's wallet within minutes

3. Operator Identification

Attribute	Detail
Name	Nathalie Roy
GitHub Username	nathroy
Repository	github.com/nicehash/xmrwallet (mirror)
Role	Sole maintainer and operator of xmrwallet.com
Activity	Active deletion of evidence, domain registration for escape sites

4. Evidence Destruction Timeline

Following public exposure of the theft mechanism, the operator engaged in systematic evidence destruction:

- **21+ GitHub issues deleted** from the repository — these contained victim reports, technical analysis of the theft mechanism, and community warnings
- Issues were deleted in bulk within hours of a PhishDestroy Research publication
- Deleted issues included screenshots, transaction hashes, and victim testimonies
- The deletion itself constitutes evidence of knowledge of the fraudulent activity

5. Escape Domain Infrastructure

After increased scrutiny, the operator registered backup domains:

Domain	Status	Purpose
xmrwallet.com	Active (primary)	Main theft operation

xmrwallet.cc	Suspended	Escape domain — taken down after abuse reports
xmrwallet.biz	Suspended	Escape domain — taken down after abuse reports

The registration of escape domains demonstrates premeditated planning to continue operations if the primary domain were disrupted.

6. Additional Indicators of Malicious Intent

VirusTotal Detection

- **6 out of 93** security vendors on VirusTotal flag xmrwallet.com as malicious
- Detections include categories: Phishing, Malware, Scam

Google Trackers in a "Privacy" Wallet

xmrwallet.com embeds **4 separate Google tracking mechanisms** in a service that markets itself as a privacy-focused Monero wallet:

1. Google Analytics (analytics.js)
2. Google Tag Manager
3. Google Ads conversion tracking
4. Google remarketing pixel

This is fundamentally incompatible with any legitimate privacy wallet and serves to profile victims for targeting.

Hidden Backdoor Endpoint

The endpoint `/support_login.html` exists on xmrwallet.com and provides a hidden administrative interface. This page is:

- Not linked from any public page on the site
- Not documented in any user-facing material
- Accessible only by direct URL entry
- Used by the operator to access stolen wallet credentials

7. Victim Impact Summary

Metric	Value
Documented victims	15+ (with evidence of significantly more)
Estimated total theft	\$2,000,000+ USD equivalent in XMR
Operational period	2016 — present (10+ years)
Average loss per victim	\$50,000 — \$200,000 USD
Recovery rate	0% — Monero transactions are irreversible

8. Indicators of Compromise (IOCs)

Domains:

- xmrwallet.com (active — primary theft operation)
- xmrwallet.cc (suspended)

- xmrwallet.biz (suspended)

Technical Indicators:

- `session_key` parameter in network requests (Base64-encoded address + viewkey)
- `raw_tx_and_hash.raw = 0` in transaction responses
- `raw_tx_and_hash.type = 'swept'` in transaction responses
- `/support_login.html` hidden endpoint
- Google Analytics/Tag Manager/Ads/Remarketing embedded in wallet pages

GitHub:

- github.com/nicehash/xmrwallet (operator repository)
- GitHub user: [nathroy](#) (Nathalie Roy)

9. Recommended Safe Alternatives

Users seeking legitimate Monero wallets should use only the following:

Wallet	Type	Verified
Feather Wallet	Desktop (recommended)	Open source, audited
Cake Wallet	Mobile	Open source, reputable
Monero GUI	Official desktop client	Maintained by Monero Project
MyMonero	Web / Desktop / Mobile	Created by Monero co-founder

Critical Rule: Never enter your Monero seed phrase or private keys into any web wallet not listed above.

10. Conclusion

The evidence presented in this report establishes beyond reasonable doubt that xmrwallet.com is a deliberately constructed theft operation. The combination of private view key exfiltration via the `session_key` mechanism, server-side transaction replacement returning `raw = 0` and `type = 'swept'`, systematic evidence destruction (21+ deleted GitHub issues), escape domain registration, hidden backdoor endpoints, and invasive tracking in a purported privacy tool constitutes a comprehensive fraud operation that has caused substantial financial harm to cryptocurrency users over a period of nearly a decade.

Report prepared by PhishDestroy Research — February 2026 Classification: PUBLIC — For widest possible distribution

Contact: <https://phishdestroy.com>