xmrwallet.com — Deleted Evidence Timeline

PhishDestroy Research — February 2026

Overview

This document provides a comprehensive timeline of evidence deletion by the operator of xmrwallet.com (Nathalie Roy, GitHub: nathroy). Following public exposure of the theft mechanism, the operator systematically destroyed evidence including GitHub issues containing victim reports, technical analyses, and community warnings. **21+ GitHub issues were deleted** in an attempt to suppress documentation of the fraud.

The act of deletion itself constitutes powerful evidence of guilt — a legitimate service operator would address user complaints, not erase them.

Summary of Deleted Materials

Category	Count	Description
Victim loss reports	8+	Users reporting stolen funds with TX hashes and amounts
Technical analyses	5+	Community researchers documenting the session_key and raw_tx theft mechanisms
Community warnings	4+	Users warning others about the scam based on personal experience
Feature requests / complaints	4+	Issues that indirectly revealed the fraudulent nature of the service
Total deleted issues	**21+**	Bulk deletion following PhishDestroy publication

Detailed Deletion Timeline

Phase 1: Early Victim Reports (2016–2022)

During this period, individual victims posted GitHub issues reporting lost funds. These issues remained visible but received no meaningful response from the operator. Examples of issues that existed during this period:

- Users reporting that their entire wallet balance disappeared after a single transaction
- Reports of transactions showing as "confirmed" but funds never arriving at the intended destination
- Complaints about the wallet showing a zero balance after previously displaying correct amounts
- Questions about unexpected `session_key` parameters observed in browser developer tools

Operator response during this phase: Silence, occasional dismissive replies suggesting "user error" or "blockchain confirmation delays."

Phase 2: Technical Exposure (2023–2025)

Independent security researchers began publishing technical analyses of the theft mechanism:

- **session_key decoding:** Researchers demonstrated that the Base64-decoded `session_key` contained the user's full Monero address concatenated with their private view key
- **raw_tx_and_hash analysis:** Transaction interception was documented by comparing the `raw` field (value: `0`) and `type` field (value: `swept`) against legitimate Monero transaction responses

- **Network traffic capture:** Complete PCAP recordings showing the exfiltration of wallet credentials to xmrwallet.com servers
- **Operator identification:** Nathalie Roy (nathroy) identified as sole maintainer through GitHub commit history, domain registration records, and code signatures

These findings were posted as GitHub issues on the xmrwallet repository, creating a permanent public record of the fraud.

Phase 3: Mass Deletion Event (Post-Exposure)

Following the publication of a comprehensive PhishDestroy Research report and increased community attention:

The operator deleted 21+ GitHub issues in rapid succession.

The deletion targeted:

Priority of Deletion	Content Type	Reason for Targeting
Highest	Technical analyses with code proof	Directly proved theft mechanism
High	Victim reports with TX hashes	Provided verifiable on-chain evidence
Medium	Community warnings	Discouraged new victims from using the service
Lower	General complaints	Indirectly supported the fraud narrative

Key observations about the deletion:

1. **Bulk timing** — Issues were deleted within a short window, indicating a deliberate cleanup operation rather than routine moderation
2. **Selective targeting** — The most technically damaging issues (those containing `session_key` decoding proof and `raw_tx_and_hash` analysis) were deleted first
3. **No explanation** — No public statement or justification was provided for the deletions
4. **Continued operation** — The service remained active after deletion, indicating intent to continue the fraud with a "clean" public record

---

Phase 4: Escape Domain Registration

Concurrent with or shortly after the mass deletion event, the operator registered backup domains:

Event	Domain	Outcome
Escape domain registered	xmrwallet.cc	Subsequently **suspended** after abuse reports
Escape domain registered	xmrwallet.biz	Subsequently **suspended** after abuse reports

The registration of escape domains simultaneous with evidence destruction demonstrates awareness that the primary operation was compromised and pre-planning for continuity of the fraud.

Evidence Preservation

Despite the operator's deletion efforts, the following evidence has been preserved:

Evidence Type	Preservation Method

GitHub issue content	Web Archive (Wayback Machine) snapshots captured before deletion
GitHub issue content	Screenshots taken by researchers before deletion
GitHub issue content	Local clones of issue data via GitHub API
Transaction hashes	Permanently recorded on the Monero blockchain
session_key samples	Captured in network traffic logs by researchers
raw_tx_and_hash samples	Documented in multiple independent research reports
Domain registration records	WHOIS history preserved by third-party services
VirusTotal detections	Archived detection results (6/93 vendors)
Google tracker evidence	Page source archives showing 4 Google tracking scripts
support_login.html	Archived copies of the hidden backdoor endpoint

---

Legal Significance of Evidence Destruction

The systematic deletion of GitHub issues constitutes:

1. **Consciousness of guilt** — The operator deleted evidence only after it was identified as proving fraud, demonstrating knowledge that the evidence was incriminating
2. **Obstruction** — Deliberate destruction of evidence that victims and law enforcement could use in investigations
3. **Ongoing fraud** — By removing warnings, the operator enabled continued victimization of new users who could no longer find the public reports
4. **Pattern of deception** — Combined with the escape domains, the deletion forms part of a broader pattern of concealment and continuation

---

Recommendations

1. **Law enforcement** should request GitHub's records of deleted issues, as GitHub retains deletion logs and content backups
2. **Victims** should reference the Web Archive snapshots as evidence in any legal proceedings
3. **Researchers** should continue archiving all publicly visible evidence on xmrwallet.com, as further deletions are likely
4. **Hosting providers and registrars** should be notified of the evidence destruction pattern when evaluating abuse reports

---

Report prepared by PhishDestroy Research — February 2026 Classification: PUBLIC — For widest possible distribution Contact: https://phishdestroy.com