THREAT INTELLIGENCE REPORT

The End of xmrwallet[.]com: NameSilo Lied to Protect a $2M Thief

Ref. **PD-TI-2026-10254** Published **10 July 2026** Source **phishdestroy.io/xmrwallet-namesilo-exposed**

Investigation Report — Final

After 10 years of stealing Monero private keys, the operation is destroyed. Three registrars acted within days. The fourth — NameSilo — contacted the scammer, believed his story, and became his press secretary.

March 27, 2026 PhishDestroy Research 12 min read

Investigation overview: The fall of xmrwallet[.]com and NameSilo's role in protecting the scammer.

$2M+

Estimated Stolen

10

Years Active

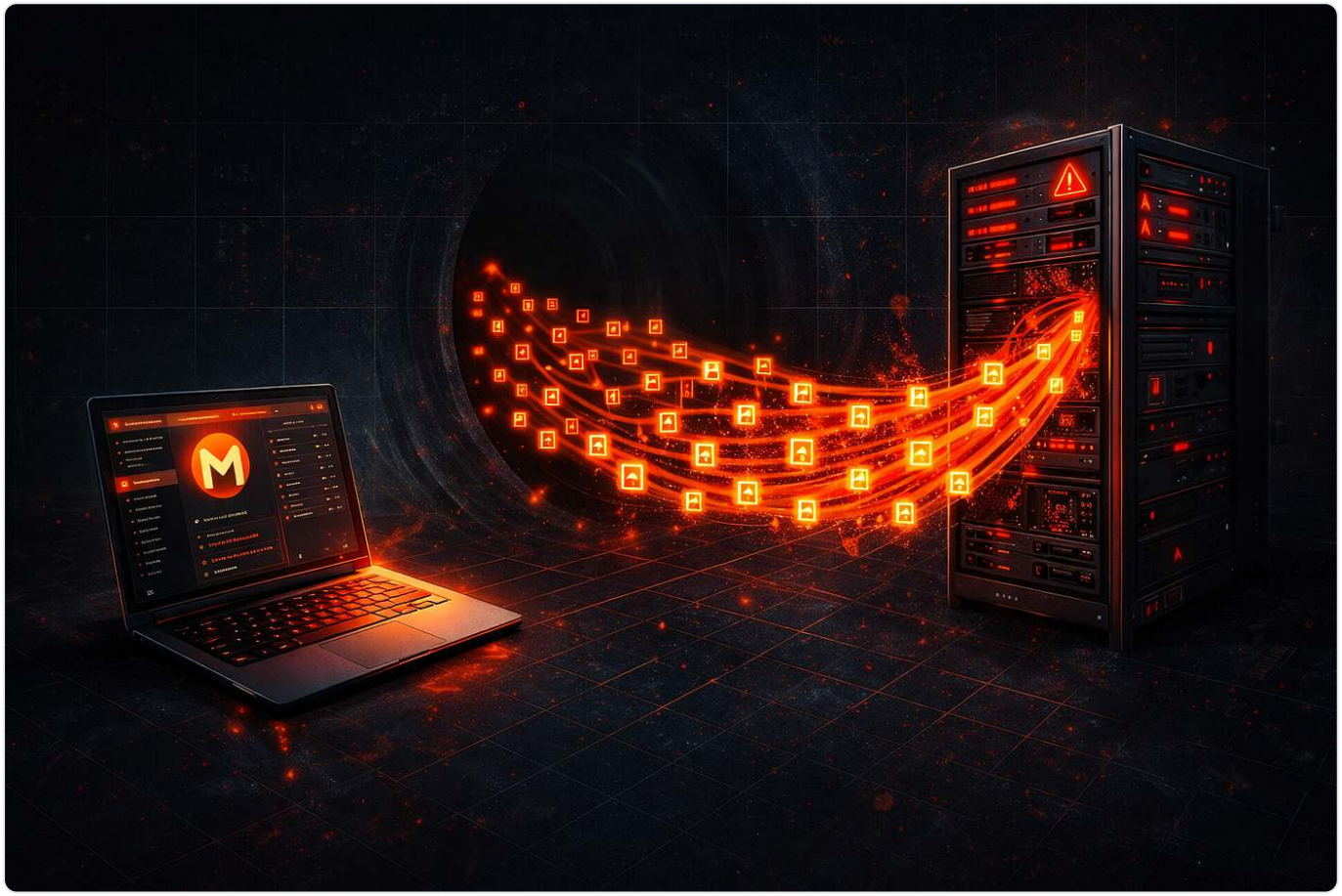
3/4

Registrars Suspended

7
NameSilo Lies Proven
8
Theft PHP Endpoints

What xmrwallet[.]com Actually Did

Since 2016, xmrwallet[.]com marketed itself as a free, open-source Monero wallet. Our **live network capture on February 18, 2026** proved it was doing something very different: stealing private Monero view keys on every login and hijacking transactions server-side.

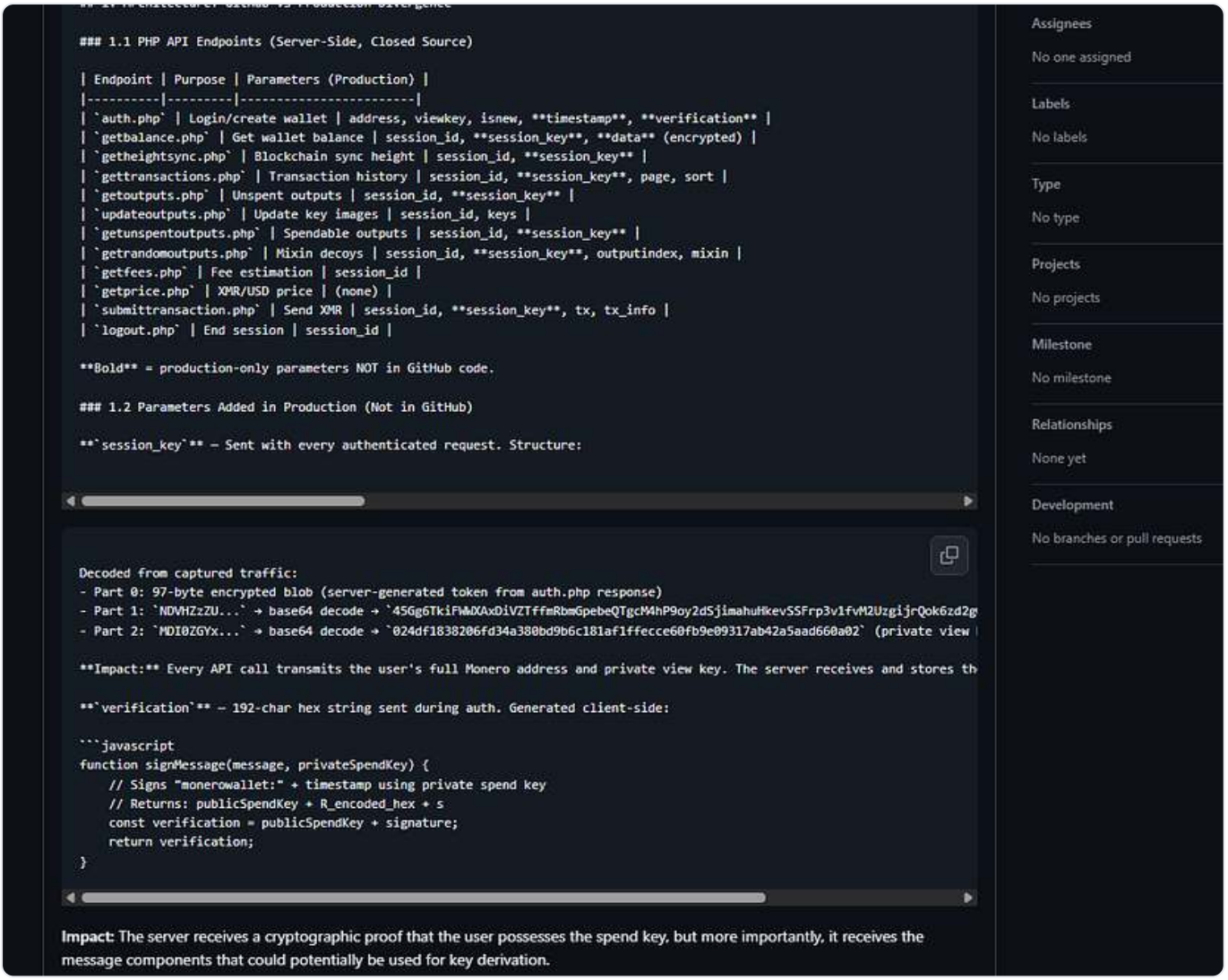


Screenshot 1 — The theft mechanism: every wallet login transmitted the victim's private Monero view key to the scammer's server via Base64 encoding.

Core Theft Mechanism

Not injected code — the **core architecture** . A session system across 8 PHP endpoints, transmitting the victim’s private view key **40+ times per session** . When users sent XMR, their transaction was silently discarded (`raw_tx_and_hash.raw = 0`) and replaced with the scammer’s.

User opens wallet
View key exfiltrated (Base64)
TX hijacked server-side
XMR sent to scammer



1.1 PHP API Endpoints (Server-Side, Closed Source)

Endpoint	Purpose	Parameters (Production)
`auth.php`	Login/create wallet	address, viewkey, isnew, **timestamp**, **verification**
`getbalance.php`	Get wallet balance	session_id, **session_key**, **data** (encrypted)
`getheightsync.php`	Blockchain sync height	session_id, **session_key**
`gettransactions.php`	Transaction history	session_id, **session_key**, page, sort
`getoutputs.php`	Unspent outputs	session_id, **session_key**
`updateoutputs.php`	Update key images	session_id, keys
`getunspentoutputs.php`	Spendable outputs	session_id, **session_key**
`getrandomoutputs.php`	Mixin decoys	session_id, **session_key**, outputindex, mixin
`getfees.php`	Fee estimation	session_id
`getprice.php`	XMR/USD price	(none)
`submittransaction.php`	Send XMR	session_id, **session_key**, tx, tx_info
`logout.php`	End session	session_id

Bold = production-only parameters NOT in GitHub code.

1.2 Parameters Added in Production (Not in GitHub)

`session_key` — Sent with every authenticated request. Structure:

Decoded from captured traffic:
- Part 0: 97-byte encrypted blob (server-generated token from auth.php response)
- Part 1: `NDVHZzZU...` → base64 decode → `45Gg6TkiFWWDXAxDiVZTffmRbmGpebeQTgcM4hP9oy2dSjimahuHkevSSFrp3v1fvM2UzgijrQok6zd2g
- Part 2: `MDI0ZGYx...` → base64 decode → `024df1838206fd34a380bd9b6c181af1ffecce60fb9e09317ab42a5aad660a02` (private view

Impact: Every API call transmits the user's full Monero address and private view key. The server receives and stores th

`verification` — 192-char hex string sent during auth. Generated client-side:

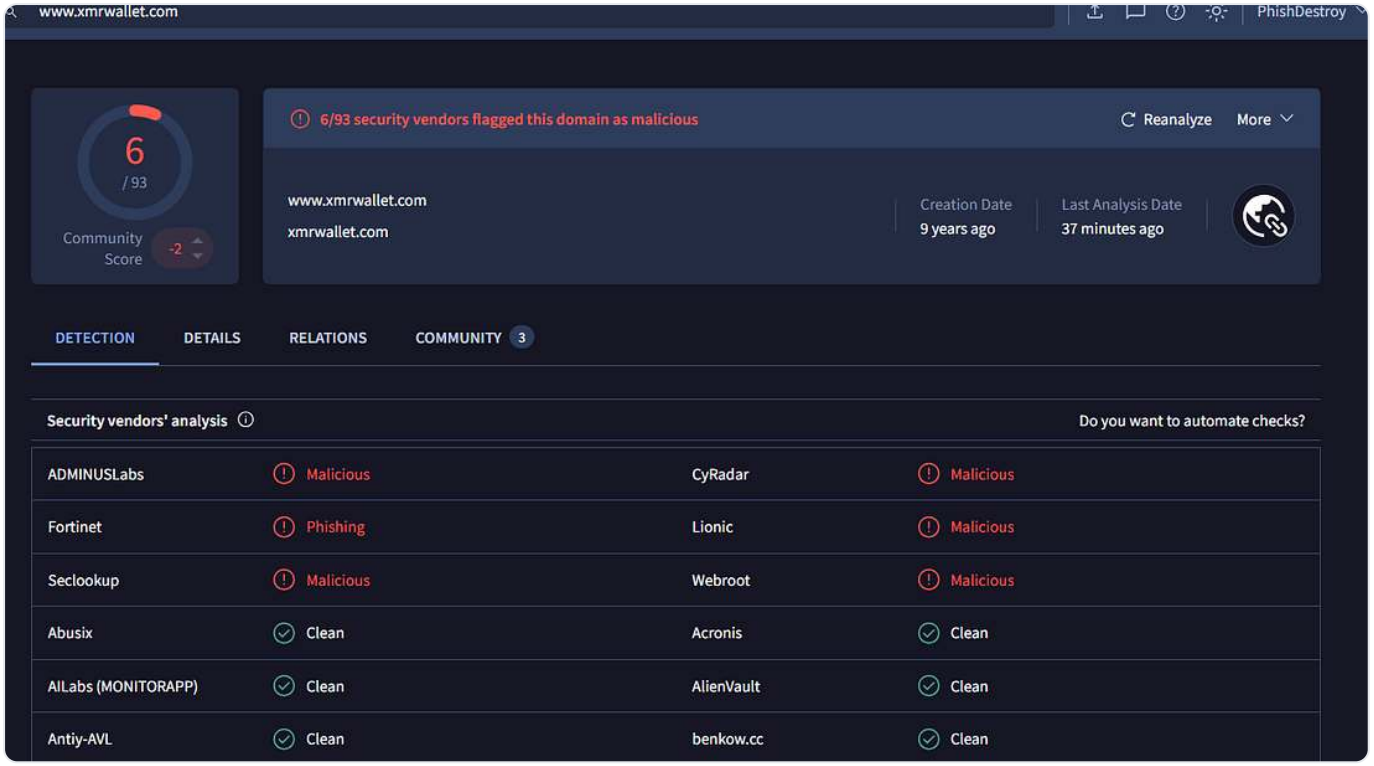
```javascript
function signMessage(message, privateSpendKey) {
    // Signs "monerowallet:" + timestamp using private spend key
    // Returns: publicSpendKey + R_encoded_hex + s
    const verification = publicSpendKey + signature;
    return verification;
}
```

Impact: The server receives a cryptographic proof that the user possesses the spend key, but more importantly, it receives the message components that could potentially be used for key derivation.

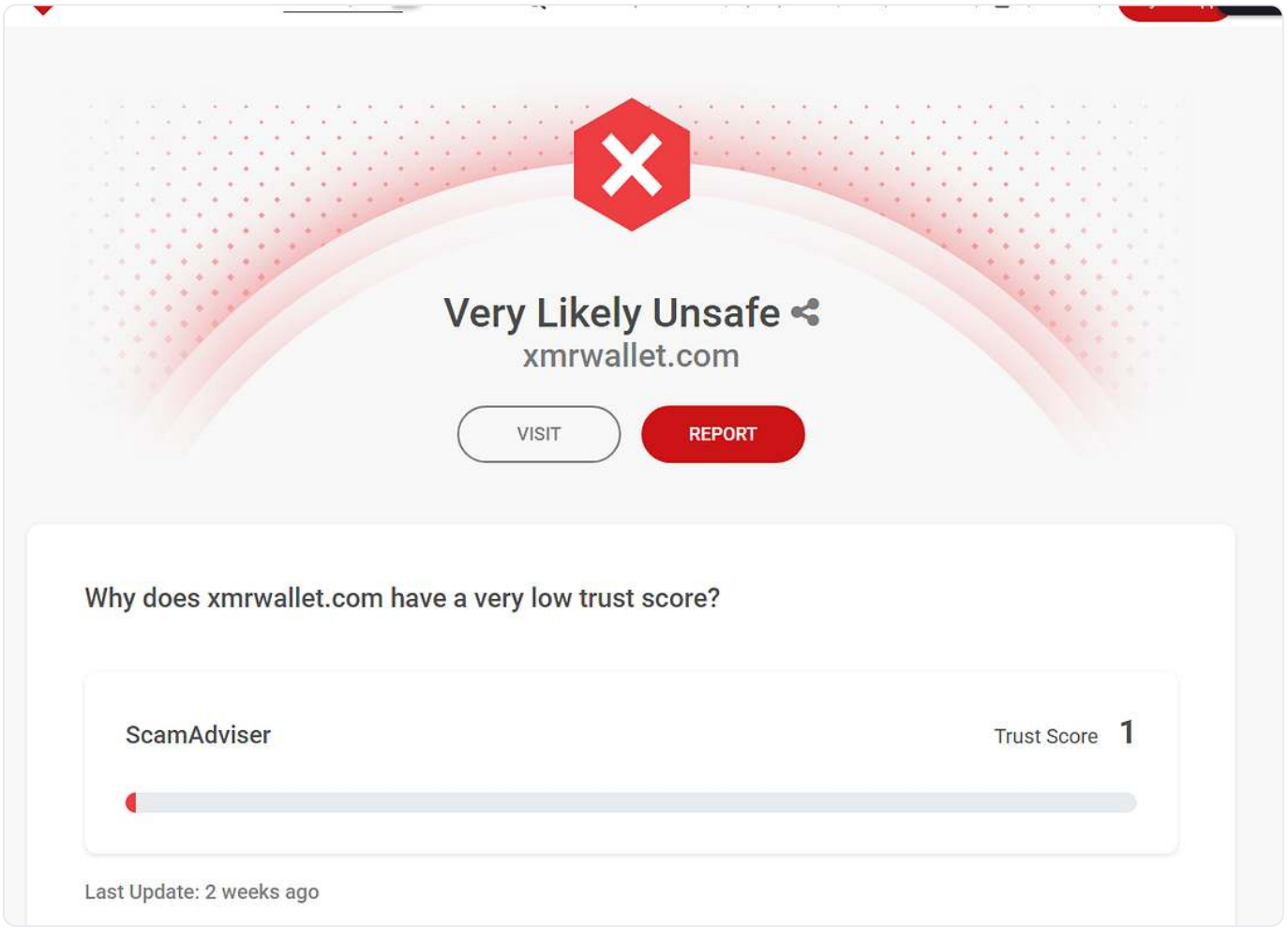
Assignees
No one assigned
Labels
No labels
Type
No type
Projects
No projects
Milestone
No milestone
Relationships
None yet
Development
No branches or pull requests

Screenshot 2 — The 8 PHP endpoints documented in our GitHub evidence repository. Each endpoint participates in the session_key/view_key exfiltration chain.

Six security vendors on VirusTotal flagged it as malicious. Fifteen documented victims across Trustpilot, Sitejabber, and BitcoinTalk. One victim lost **590 XMR (~$177,000)** in a single theft.



Screenshot 3 — VirusTotal: 6/93 vendors flagged xmrwallet.com as malicious. Fortinet classified it as “Phishing.”



Screenshot 4 — ScamAdviser: Trust Score 1/100. “Very Likely Unsafe.”

Three Registrars Did Their Job

We filed identical abuse reports with all four registrars hosting xmrwallet domains. Three acted immediately:

Screenshot 5 — Three registrars locked the doors. NameSilo left theirs wide open for the scammer.

PublicDomainRegistry

xmrwallet.cc
Suspended
India · Days to act

WebNic

xmrwallet.biz
Suspended
Malaysia · Days to act

NICENIC

xmrwallet.net
DNS Dead
China · Weeks to act

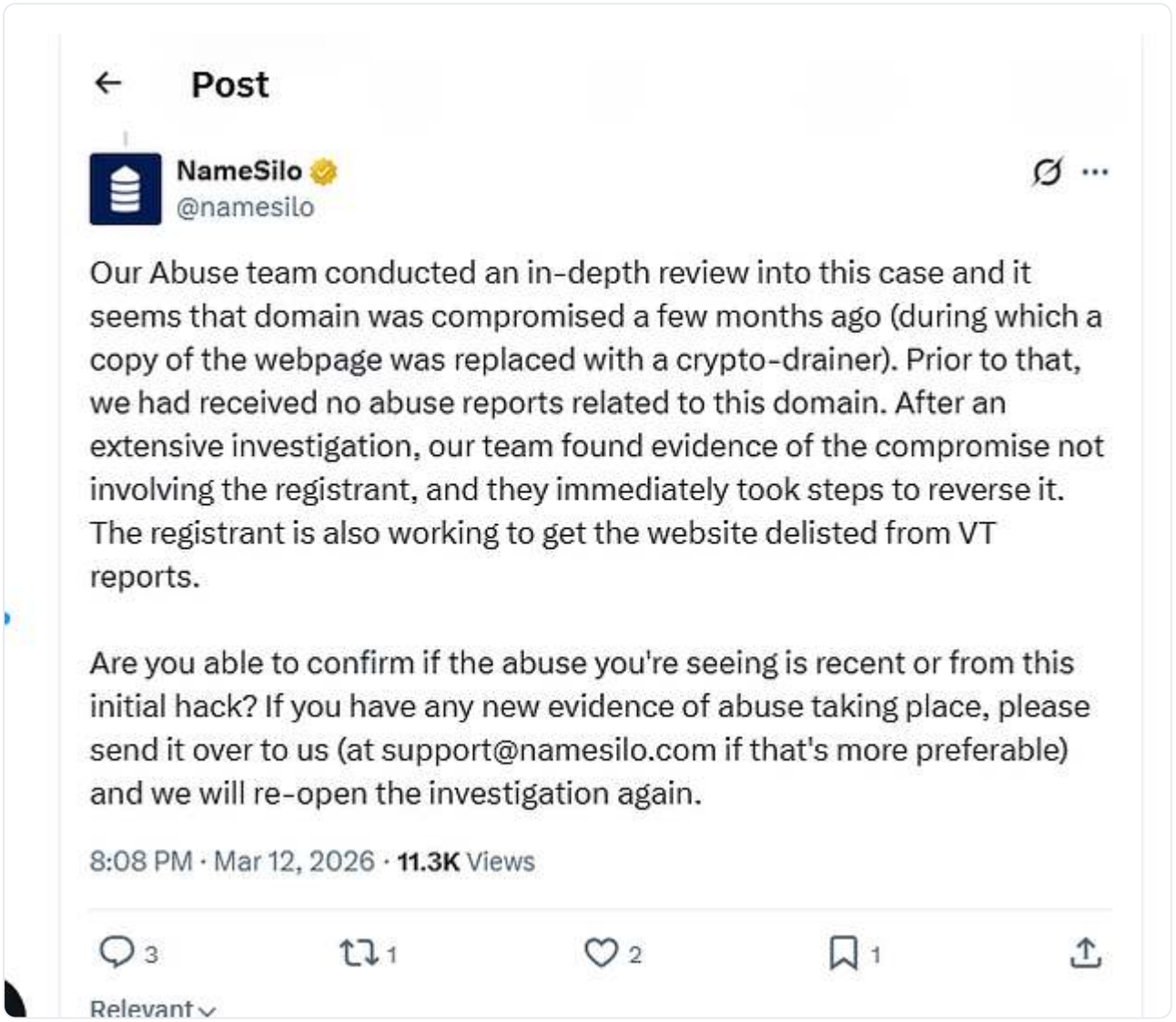
NameSilo

xmrwallet.com
Refused
USA · Defended scammer

Three countries. Three independent conclusions.
India, Malaysia, China — reviewed the evidence, found fraud, suspended the domains. No questions asked.

NameSilo Chose a Different Path

The fourth registrar — **NameSilo, LLC (USA)** — hosting the primary domain with the most evidence and most victims — did the opposite. They contacted the scammer, believed his story, and published a public statement defending him:



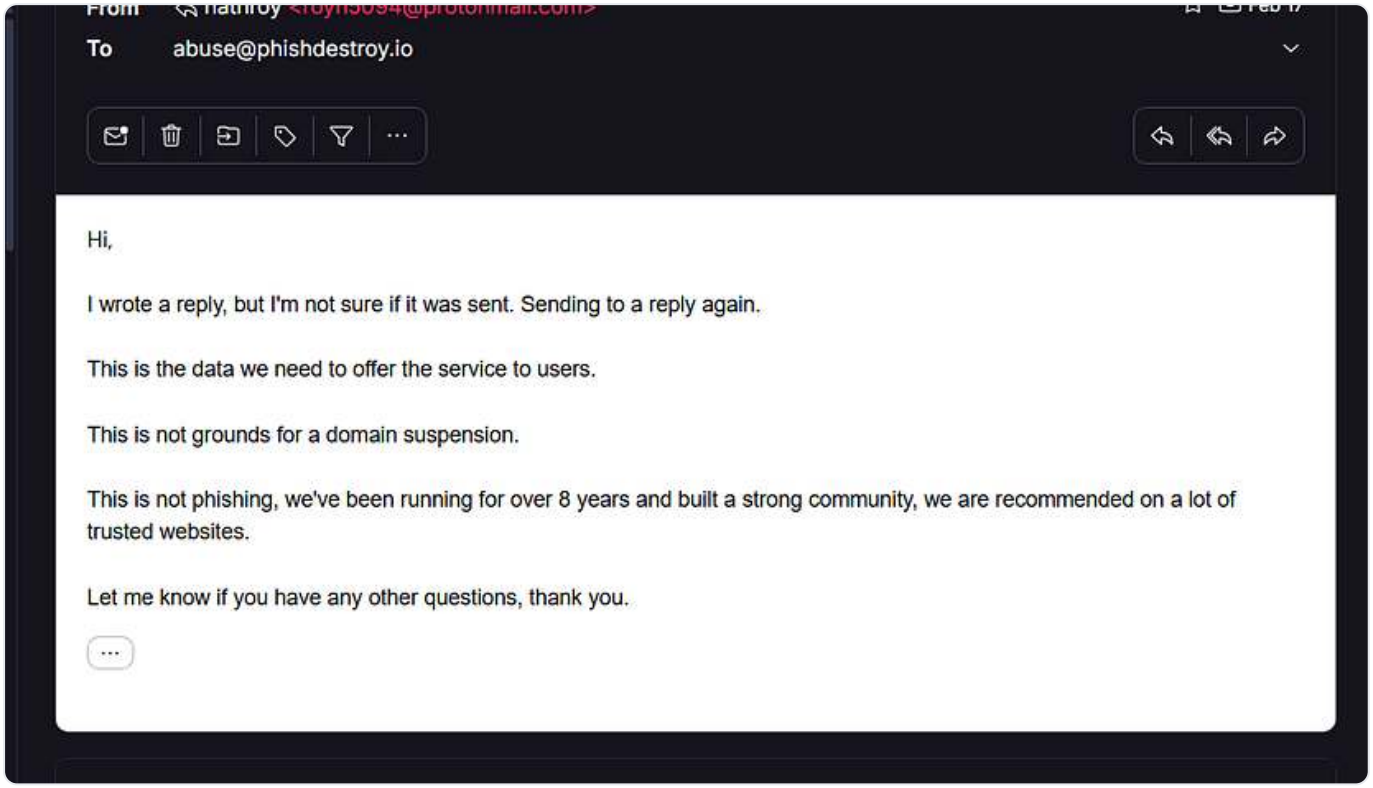
Screenshot 6 — NameSilo's public statement on X (Twitter), March 12, 2026. Every claim in this post was false.

> "Our Abuse team conducted an in-depth review into this case and it seems that domain was compromised a few months ago... After an extensive investigation, our team found evidence of the compromise not involving the registrant... The registrant is also working to get the website delisted from VT reports."
>
> — NameSilo, via X (Twitter)

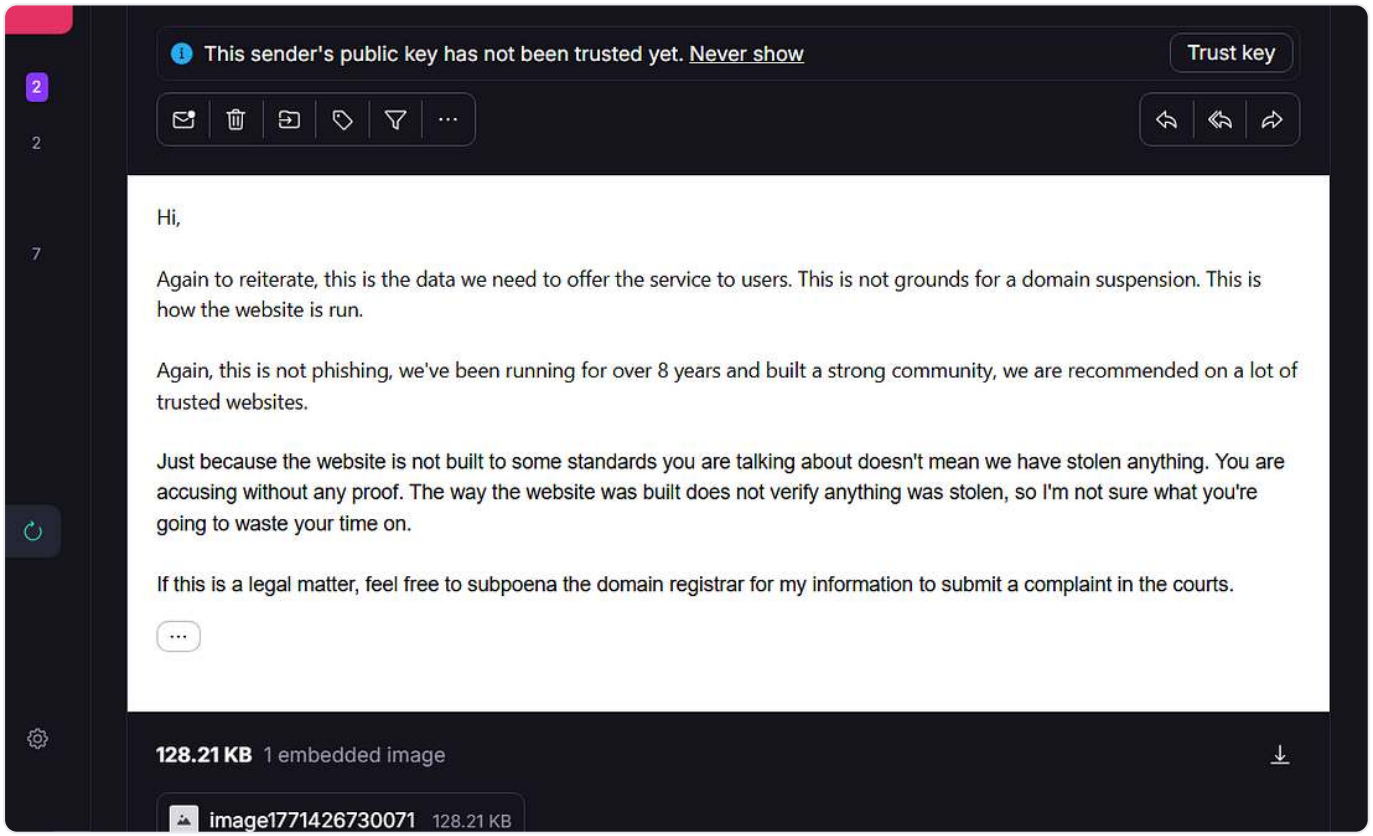
We analyzed this statement line by line. **Every claim was false.**

The Operator's Own Words

Before NameSilo intervened, the operator responded directly to our abuse report. His emails confirm awareness and intent:



Screenshot 7 — Operator's response: "This is not phishing, we've been running for over 8 years."



Screenshot 8 — Operator's second response: “This is the data we need to offer the service.” The “data” was the victim's private view key.

Seven Lies, Exposed

LIE #1: “The domain was compromised”
The theft mechanism is the core architecture — 8 PHP endpoints, Base64 key exfiltration, a **5.3-year GitHub commit gap** . This system was built over years, not injected in a hack.

LIE #2: “We had received no prior abuse reports”
Six VirusTotal vendors, Trustpilot complaints going back years, a BitcoinTalk warning thread, the operator **banned from r/Monero in 2018** . A single Google search would have shown this.

LIE #3: “Not involving the registrant”
The operator registered **4 escape domains across 4 registrars** (prepaid 5-10 years each) *before* the investigation was published. Deleted 21+ GitHub issues. Hired developers for a captcha system. That’s not a victim — that’s an operation.

LIE #4: “They immediately took steps to reverse it”
The theft code was running in production **during NameSilo’s statement** . Zero GitHub commits addressing any incident. Nothing was reversed.

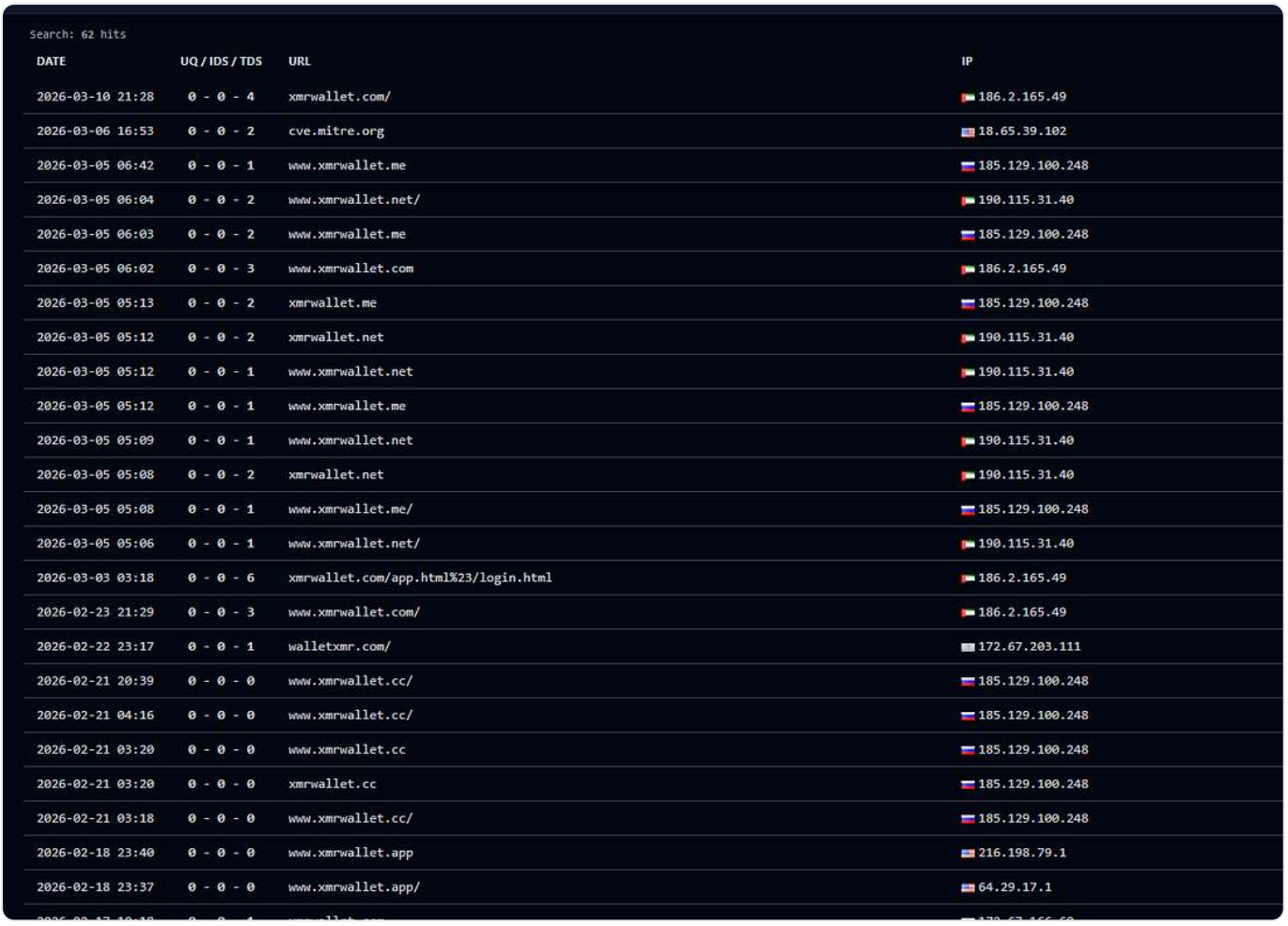
LIE #5: “Working to get delisted from VirusTotal”
NameSilo praised the scammer for lobbying to remove Fortinet’s “Phishing” detection — **without removing the phishing code** . That’s not good faith. That’s suppressing security warnings.

LIE #6: “Is the abuse recent?”
Shifting the burden of proof to the reporter so they can close the case. The evidence was in the report. Three peer registrars didn’t need to ask.

LIE #7: “We will re-open the investigation”
“Re-open” implies it was once open. Their investigation consisted of calling the scammer and writing down what he said. That’s not an investigation — that’s dictation.

Infrastructure Evidence

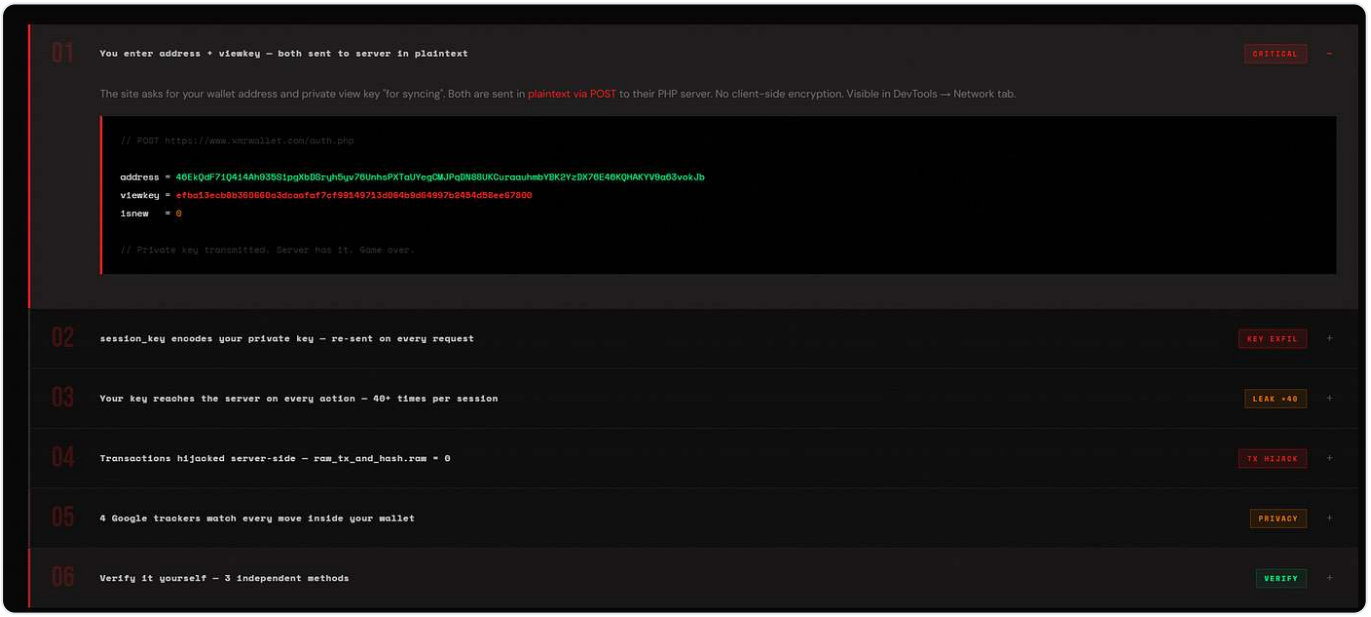
Screenshot 9 — The domain escape network: 4 domains across 4 registrars, all pointing to the same servers. Three neutralized.



Search: 62 hits

DATE	UQ / IDS / TDS	URL	IP
2026-03-10 21:28	0 - 0 - 4	xmrwallet.com/	186.2.165.49
2026-03-06 16:53	0 - 0 - 2	cve.mitre.org	18.65.39.102
2026-03-05 06:42	0 - 0 - 1	www.xmrwallet.me	185.129.100.248
2026-03-05 06:04	0 - 0 - 2	www.xmrwallet.net/	190.115.31.40
2026-03-05 06:03	0 - 0 - 2	www.xmrwallet.me	185.129.100.248
2026-03-05 06:02	0 - 0 - 3	www.xmrwallet.com	186.2.165.49
2026-03-05 05:13	0 - 0 - 2	xmrwallet.me	185.129.100.248
2026-03-05 05:12	0 - 0 - 2	xmrwallet.net	190.115.31.40
2026-03-05 05:12	0 - 0 - 1	www.xmrwallet.net	190.115.31.40
2026-03-05 05:12	0 - 0 - 1	www.xmrwallet.me	185.129.100.248
2026-03-05 05:09	0 - 0 - 1	www.xmrwallet.net	190.115.31.40
2026-03-05 05:08	0 - 0 - 2	xmrwallet.net	190.115.31.40
2026-03-05 05:08	0 - 0 - 1	www.xmrwallet.me/	185.129.100.248
2026-03-05 05:06	0 - 0 - 1	www.xmrwallet.net/	190.115.31.40
2026-03-03 03:18	0 - 0 - 6	xmrwallet.com/app.html%23/login.html	186.2.165.49
2026-02-23 21:29	0 - 0 - 3	www.xmrwallet.com/	186.2.165.49
2026-02-22 23:17	0 - 0 - 1	walletxmr.com/	172.67.203.111
2026-02-21 20:39	0 - 0 - 0	www.xmrwallet.cc/	185.129.100.248
2026-02-21 04:16	0 - 0 - 0	www.xmrwallet.cc/	185.129.100.248
2026-02-21 03:20	0 - 0 - 0	www.xmrwallet.cc	185.129.100.248
2026-02-21 03:20	0 - 0 - 0	xmrwallet.cc	185.129.100.248
2026-02-21 03:18	0 - 0 - 0	www.xmrwallet.cc/	185.129.100.248
2026-02-18 23:40	0 - 0 - 0	www.xmrwallet.app	216.198.79.1
2026-02-18 23:37	0 - 0 - 0	www.xmrwallet.app/	64.29.17.1

Screenshot 10 — URLScan data: all xmrwallet domains (.com, .cc, .biz, .net, .me, .app) resolving to the same infrastructure.



Screenshot 11 — Our GitHub evidence repository with the complete network capture analysis. 109 requests, 43 view key transmissions documented in a single session.

Timeline: The Fall of xmrwallet

2016

xmrwallet[.]com begins operation, marketing as “free open-source Monero wallet”
2018
Operator **banned from r/Monero** . First victim reports appear on Trustpilot
Feb 4, 2026
Escape domain xmrwallet.cc registered (8yr prepaid) — *before investigation published*
Feb 13, 2026
Issue #35 published — full TX hijacking mechanism exposed
Feb 18, 2026
Issue #36 — live capture: 109 requests, 43 viewkey transmissions in single session
Feb 23, 2026
xmrwallet.cc SUSPENDED (PDR). **xmrwallet.biz SUSPENDED** (WebNic). Operator panic-deletes Issues #35 & #36
Feb 26, 2026
More panic: xmrwallet.net and .me registered (10yr prepaid, same IPs as suspended domains)
Mar 8, 2026
xmrwallet.net DNS DEAD (NICENIC). 3 of 4 escape domains neutralized
Mar 2026
NameSilo publishes statement: **“The registrant is the victim.”** Helps suppress VirusTotal detections
Mar 27, 2026
Formal ICANN complaint filed (RAA Section 3.18). Evidence submitted to law enforcement. This report published.

The Verdict

NameSilo didn’t ignore the evidence. They read it, called the scammer, believed him, declared him innocent, and helped suppress security warnings. Then asked the researchers to prove the abuse is “recent.”

That’s not negligence. That’s a partnership.

The domain is down. The scam is over. But the fact that a US registrar chose to publicly fabricate a cover story to shield a $2M crypto thief — that is something that will follow NameSilo for a very long time. Their statement will be Exhibit A in every filing from this point forward.

If you vouch for the thief, you share his bill.

Evidence & Resources

Related Investigations

This investigation is based on publicly available evidence, live network captures, OSINT, public review platforms, and NameSilo’s own verbatim public statement. No unauthorized access was performed. All findings are independently reproducible.