THREAT INTELLIGENCE REPORT

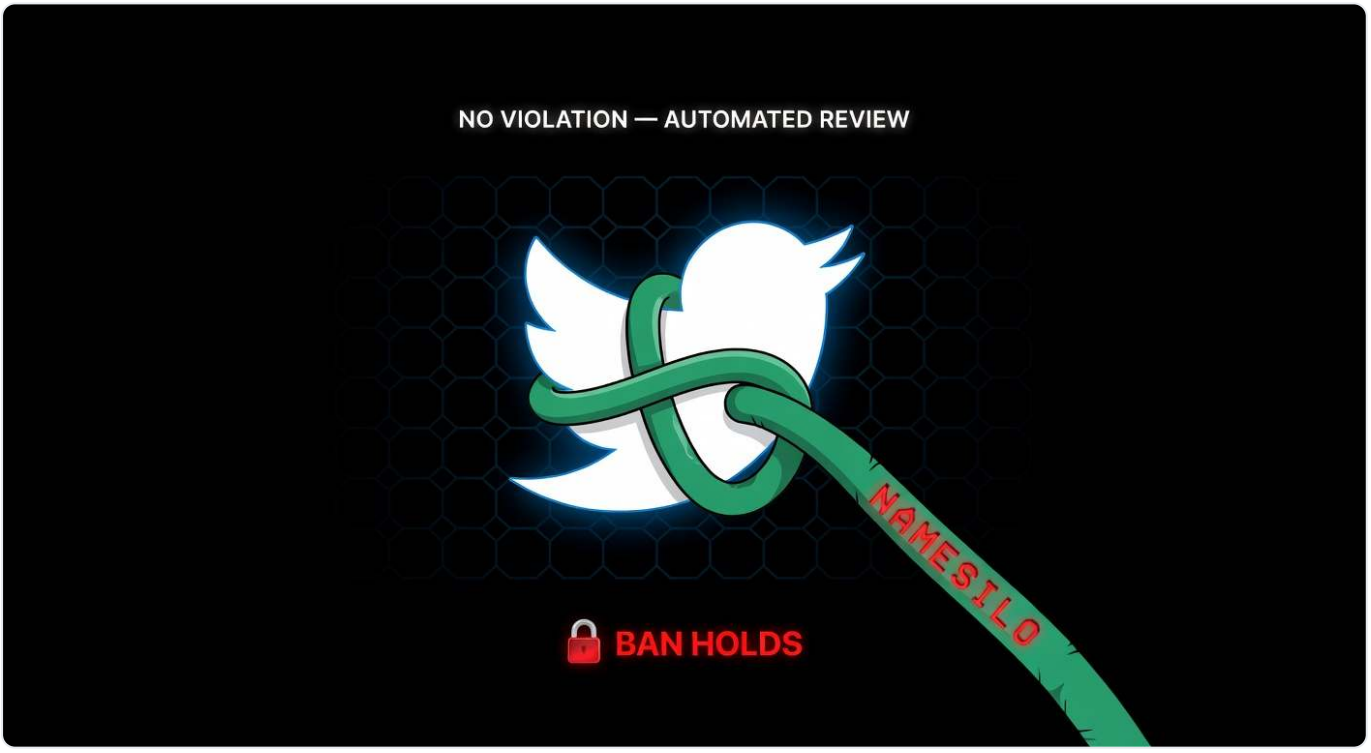
NameSilo Killed Our Twitter Because We Told the Truth About Them

Ref. **PD-TI-2026-32715** Published **10 July 2026** Source **phishdestroy.io/namesilo-killed-our-twitter**

Retaliation Report

On **April 3, 2026** , X locked **two PhishDestroy accounts** citing a “payment issue,” with a promise that the paid subscriptions would be refunded. No refund arrived. **Eleven days later, on April 14** , X issued a new justification: *“inauthentic behaviors — overturn not warranted.”* We appealed. X’s own automation answered in writing: *“no violation — account restored to full functionality.”* **The accounts are still locked. The money is still not refunded. The stated reason has now changed three times. Two weeks earlier we exposed NameSilo sheltering a $20M+ Monero-theft operation — now under active EU criminal investigation.**

April 15, 2026 PhishDestroy Research 9 min read



The ban visualized: X’s own automation cleared the account. A human-routed NameSilo complaint kept it killed anyway.

Reason #1 · Apr 3

“Payment issue” + refund promised.

Two accounts locked. Subscriptions were paid and active. Refund never arrived.

Reason #2 · Apr 14

“Inauthentic behaviors.”

Eleven days later, a completely new justification. No specific tweet cited. No evidence disclosed.
Reason #3 · After appeal
“No violation — restored.”
Appeal result. X’s latest official ruling: the accounts are cleared.
Reality · Today
Accounts locked. Money gone.
Three different reasons. One unchanged outcome. No refund. No restored access.
0
Violations on appeal
10
Years sheltered
$20M+
Confirmed losses
~$100M
Our estimate
7
NameSilo lies
1
Paid checkmark

The Receipts: X Contradicts Itself in Writing

Two official emails from X Support. Same account. Same appeal. Opposite rulings. The second one is the more recent. Read them in order.

The contradiction visualized: X's automated review cleared us in writing. The ban held anyway.

Email #1 · April 3 · Initial lock decision

𝕏

Hello,

We have reviewed your appeal request for account, **@Phish_Destroy** .

Our support team has determined that a violation of our Rules did take place, specifically:

Violating our Rules against inauthentic behaviors .

We considered the additional information provided and **decided an overturn of our original decision is not warranted in this case** . Therefore, we will not overturn our decision to lock your account.

Thanks,
X Support

Lock justification: **“INAUTHENTIC BEHAVIORS”**

Email #2 · After our appeal · Automated review

𝕏

Hello,

We have reviewed your appeal request for account, **@Phish_Destroy** .

Our automated systems have determined there was no violation and have restored your account to full functionality.

Thanks,
X Support

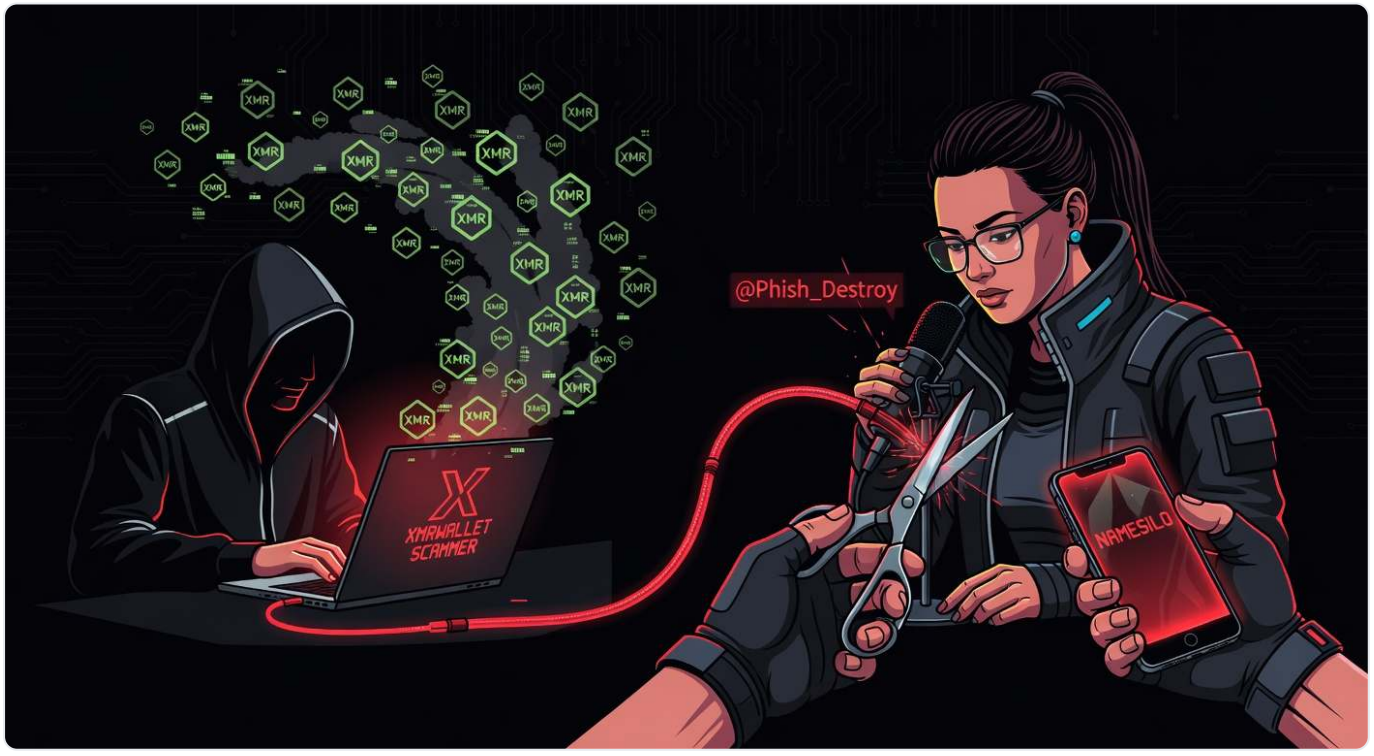
Appeal result: **“NO VIOLATION — RESTORED”**
Email #2 is the more recent ruling. It explicitly reverses Email #1. It says — in writing, on X’s own letterhead — that the account has been **restored to full functionality** . The account is not restored. The paid subscription continues to bill. There is no third email walking back Email #2. X’s most recent commitment to us is simply not being honored.

Two possibilities. Both bad.
Either Email #2 is real — automation reviewed the appeal, concluded no violation, and some unnamed party is keeping the ban in place against that ruling.

Or Email #2 is not real — it was sent in error, the real decision is still Email #1, and X has not issued a correction in writing.

There is no third possibility. Both reflect poorly on X. One of them reflects catastrophically.

Why This Happened



One hand. Two protections. One for the scammer. One silencing the researcher who caught them.

On March 27 we published *The End of xmrwallet[.]com: NameSilo Lied to Protect a Crypto Thief* . The investigation was reproducible: PHP endpoint dumps, archived statements, 15+ documented victims. Three peer registrars (India, Malaysia, China) reviewed the same evidence and killed their `xmrwallet` domains in days. Only NameSilo defended the scammer.

What happened next matters. The order matters:

1. **The scammer emailed us directly first** — before any NameSilo public statement, before any appeal was filed. His email told us to "sue the registrar." That is not a sentence a solo scammer writes to a researcher chasing him. That is a sentence someone writes when they already know the registrar will back them up. **We have never seen that reaction from any other scammer we have documented.**
2. **NameSilo then issued a public statement** containing two provable falsehoods, quoted verbatim and archived in our Medium investigation :
   • *"Domain was compromised a few months ago"* — contradicted by the fact that the operator's own theft code was still running in production at the time of NameSilo's statement.
   • *"Prior to that, we had received no abuse reports"* — contradicted by our delivery receipts for multiple prior abuse reports with full technical evidence.
   The same statement also said: *"Registrant is working to get delisted from VT reports,"* which confirms NameSilo explicitly endorsed the operator's attempt to remove VirusTotal detections while the theft code was live.
3. **In the same statement** , NameSilo dismissed our research as unserious *and* publicly offered to help the operator get security-vendor detections (VirusTotal, Fortinet) removed — while the theft code was still active.
4. We **responded factually** to that public statement. No harassment. No spam. No doxing. We corrected the record in the same venue NameSilo chose.
5. Seven days later, **two PhishDestroy X accounts were locked** . Reason cited: "payment." Subscriptions were paid. The reason shifted on Apr 14 to "inauthentic behaviors." After appeal the reason shifted again to "no violation, restored." The lock, and the unreturned payments, did not shift at all.

The pattern identifying the real reason
NameSilo couldn't refute the evidence — three peer registrars acted on it independently. So they did what the `xmrwallet` operator had been doing to critics for ten years: **used a bureaucratic channel to silence the voice, without addressing the facts** . The operator deleted 20+ GitHub accounts and 200+ Trustpilot reviews. NameSilo got an X account banned. Same playbook, corporate-grade.

Are NameSilo and the Scammer Connected?

The `xmrwallet[.]com` operator answered abuse reports with confidence, tweeted alongside the registrar with coordinated talking points, and never moved the domain in ten years of complaints. That is not how nervous scammers behave. That is how scammers with an arrangement behave.

In more than a hundred phishing-operator cases we've documented, we have never seen this specific sequence before:

The sequence we have never seen with any other scammer

1. **The scammer wrote to us first.** Before NameSilo made any public statement, before any appeal was filed — the operator himself emailed PhishDestroy. Identity is documented in the Medium investigation : the emails came from the `xmrwallet[.]com` operator, publicly identifiable via his own repository footprint as **Nathalie Roy** (Canada), GitHub `nathroy` , Reddit `u/WiseSolution` , banned from `r/Monero` in 2018.
2. **His exact words (verbatim, archived):** *"Feel free to subpoena the domain registrar."* Not "take it down." Not "I'll fix it." He explicitly pointed us at his own registrar as a party to go after — as if he already knew the registrar would not act against him, and was confident their legal posture would survive scrutiny. This quote is preserved in our Medium investigation (March 16, 2026) .
3. **Only then did NameSilo go public** with the "our customer was hacked" cover story — a cover story contradicted by the still-running theft code — and the assertion that "no prior abuse reports existed," contradicted by our delivery receipts.
4. **NameSilo then weaponized a platform abuse channel** against us — using the same silencing playbook the operator had already been running on GitHub (20+ accounts deleted), Trustpilot (200+ reviews deleted), and BitcoinTalk.

The operator's infrastructure is not that of a hobbyist. According to our Medium investigation , `xmrwallet[.]com` is hosted on **$550/month bulletproof hosting via IQWeb FZ-LLC** (registered in **Belize**), behind **DDoS-Guard** (Russia). That is a professional, prepared, abuse-resistant stack — not a one-off scam page. A single operator running prepared bulletproof infrastructure while also having his registrar publicly issue a defense statement on his behalf is, at minimum, an unusually coordinated operation.

We cannot prove a relationship from outside NameSilo's books. Only their internal records could. But on the visible evidence, two explanations remain: either the operator is the most self-confident crypto scammer of the last decade and correctly bet that his registrar would shield him on instinct — *or* there is an undisclosed relationship between them. The first deserves public scrutiny. The second deserves a subpoena. Law enforcement in EU jurisdictions is now working the underlying case.

Direct Evidence: What NameSilo Said Publicly vs. What Actually Happened

The paragraphs above describe a pattern. This section documents the specific factual contradictions between NameSilo's public statements and our own first-hand records. We are not asking anyone to believe us on faith — every item below is verifiable against third-party archives, delivery receipts, and the Wayback Machine.

NameSilo's public line, and why it does not survive contact with our records

1. **Public claim: "no prior abuse reports existed / reports were not received within compliance windows."**
   Our record: the PhishDestroy team personally sent **more than 20 abuse notices over three years (2023–2026)** for `xmrwallet[.]com` and related infrastructure. Each submission used NameSilo's published abuse channel, generated a tracking reference, and — in multiple cases — received autoresponder confirmations that are still in our mail archive. We preserved these receipts. We will release them, in full, to any ICANN, GDPR, EU LE, or court proceeding that requests them. A registrar saying "we received nothing" after three years of *documented* complaints is not an administrative oversight. It is a provable factual misstatement.

2. **Public claim: “this was a one-off compromise; the customer was hacked.”**
   Our record: the theft code at `xmrwallet[.]com` stayed online across **ten continuous years** with the same wallet-substitution behavior, the same operator fingerprint (*Nathalie Roy / nathroy / u/WiseSolution*), and the same bulletproof stack (**$550/mo IQWeb FZ-LLC in Belize behind DDoS-Guard**). A compromise that lasts a decade and pays a steady bulletproof bill is not a compromise. It is a **business** . We personally know — and have consent to reference — **at least one individual close to our team** who lost funds on that exact domain before we began the public investigation. This is not a theoretical harm. It is a specific person.
3. **The DDoS-Guard → GitHub pivot is not credible.**
   NameSilo-aligned narratives have floated the idea that the operator’s infrastructure somehow proves he is merely a disorganized open-source contributor. A domain sitting for a decade behind a Russian bulletproof DDoS mitigation service, paid via offshore corporate structures in Belize, is not consistent with “guy with a GitHub page.” No reasonable observer — technical or not — accepts this framing. We are noting it here because silence could be mistaken for agreement.

The Scrubbing Pattern: Accounts, Not Just Comments

During our three-year investigation we watched, in real time, the suppression layer operate on three different platforms. The pattern was consistent enough that we began archiving before publishing, every time.

- **GitHub.** Entire *accounts* that posted issues or comments referencing `xmrwallet[.]com` were removed — not individual comments, not threads, the full accounts. We have Wayback captures of issue threads where the commenter’s profile now 404s. Anyone conducting an inquiry can ask GitHub, under proper legal process, how many user accounts with posts mentioning `xmrwallet` were closed between 2018 and 2026, and for what stated reason. We expect the number to be non-trivial.
- **Trustpilot.** Dozens of truthful negative reviews were removed over successive waves. The removals clustered with each public complaint cycle, consistent with coordinated reporting rather than organic moderation. Again, Trustpilot’s internal deletion log, under subpoena, is the definitive record.
- **X (Twitter).** Critical replies to the scam-adjacent accounts disappeared at a rate difficult to explain by normal platform policy. After our `@Phish_Destroy` account was ultimately banned on a shifting justification (see the email receipts above), the pattern clicked into place. The same suppression playbook used against individual complainants for years was now being run against a research account.

We want to be precise: we are not alleging telepathy. We are alleging a documented chronology. **Post. Get archived. Get deleted. Repeat, across three platforms, for the same target, for a decade, while the registrar never moves the domain.** That chronology does not require a conspiracy theory. It requires a public records request.

If You Are a Victim of `xmrwallet[.]com` — Please Come Forward

We know there are more of you. We have been contacted privately by people who lost funds and who were afraid to go on the record while the operator was still active and while his registrar was still

publicly defending him. The situation has now changed. The operation is exposed, the infrastructure is documented, and law enforcement in EU jurisdictions is working the underlying case.

If you lost funds on `xmrwallet[.]com` — three practical steps

1. **File a formal police report** in your country of residence. Reference the domain `xmrwallet[.]com` , the approximate date and amount, and the destination wallet if you have it. A police report is what unlocks exchange-side freeze requests downstream.
2. **Preserve every artifact:** screenshots, browser history, email receipts, transaction IDs, wallet addresses, approval signatures. Do not assume anything will still be online next week. Save locally *and* submit to archive.org .
3. **Tell us.** Write to report@phishdestroy.io or DM via @PhishDestroy_bot . We do not republish your identity without consent. Your testimony — even anonymously — strengthens the case against the infrastructure that enabled the theft.

To the institutions that can actually compel disclosure — ICANN Compliance, EU GDPR authorities, Canadian Anti-Fraud Centre (the operator is Canadian), the relevant tax authorities, and any court with jurisdiction over NameSilo's operating entity: the primary-source material is preserved and available on request. Delivery receipts, Wayback captures, Medium write-up, domain-report infrastructure graph, and victim testimony with signed consent. We are not holding back evidence. We are holding it in a form you can actually use.

Calling black white does not make it white. A decade of public evidence, 20+ documented abuse notices, a bulletproof-hosted theft machine, coordinated account deletions across three platforms, a banned research account, and a named operator whose identity is already public — this is not a PR problem. It is a jurisdictional problem. We are confident the public record already contains enough to resolve it.

The Victims: Who Actually Got Harmed

NameSilo's implicit argument, by reaching for a platform abuse button instead of a retraction, is "we didn't like being exposed." Fair enough. People rarely like being exposed. But put the two harms on one scale.

The asymmetry
NameSilo's harm from our reporting: embarrassment.

Victims' harm from the operation NameSilo sheltered for ten years:

- One single user: **590 XMR (~$177,000)** lost in a single hijacked transaction.
- Initial documented cases: 15 (Trustpilot, Sitejabber, BitcoinTalk).
- Regions: **different regions** (victim reports corroborate this).
- **Confirmed aggregate: $20M+.** This is based on victim reports we can individually verify.
- **Our opinion, informed but unverified: $100M+.** Based on victim outreach and operation duration. We state this as our estimate and cannot prove it publicly. NameSilo also cannot credibly deny it without opening their own records.
- **Important pricing note.** Our loss totals are calculated at the XMR exchange rate *at the time of each theft* , not at today's Monero price. The figures above are the actual USD-equivalent amounts

victims lost when they lost them.

- **Active criminal cases in EU jurisdictions.** This is no longer just research — it is law enforcement.

Since publication, **additional victims have reached out to us directly** with individual loss amounts and transaction IDs. We are preserving and corroborating those reports.

Treating these two harms as comparable — by letting a registrar silence the researcher who documented the operation — is itself a policy failure.

The Permanent Record

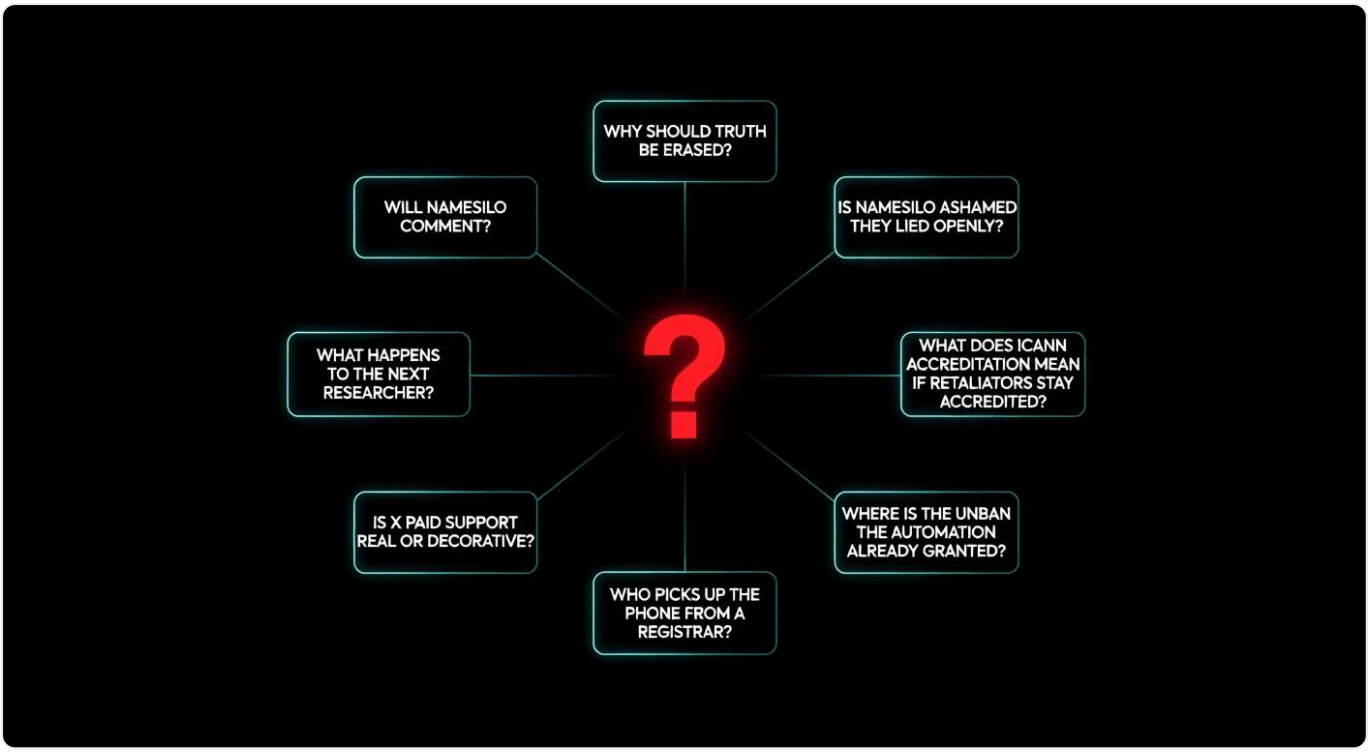
Every NameSilo statement defending the xmrwallet operator, preserved across eight independent publishing systems.

Silencing a Twitter account does not remove the evidence. Everything germane to this case is archived:

- Every public NameSilo statement defending the `xmrwallet` operator — Wayback Machine, Archive.today, our GitHub evidence repository.
- Screenshots of the live theft code in production, with timestamps.
- 8 PHP endpoints reverse-engineered and published.
- The full abuse-report conversation chain.
- Our entire X timeline mirrored on Mastodon, Bluesky, Medium, Telegram, GitHub, IPFS.
- Hourly snapshots of `phishdestroy.io` itself, 14-day retention, installed specifically so nothing we wrote can quietly disappear.

If any one mirror is silenced, the content lives on the other seven. The architecture is older than NameSilo. It will outlast them.

Was This Fair? Five Questions for Everyone Reading



Answerable questions. Every one of them deserves a public answer.

These are not rhetorical. Read the evidence above, then answer for yourself — privately, on your timeline, or while deciding whether to keep or move your domains.

1. **Is it fair to ban a security researcher for publicly responding to a registrar's own public statement?** The registrar started the conversation. The researcher replied with facts. Only one side got silenced.
2. **Is it acceptable for a registrar's public statement to dismiss documented research as unserious while simultaneously offering to help a scam operator remove security detections?** Both happened in one NameSilo statement. Victims are not mentioned anywhere in it.
3. **Is it acceptable for X to explicitly withdraw its own lock justification in writing ("no violation, restored") and keep the ban in force anyway?** X's own most recent ruling says the account should be live.
4. **Is it acceptable for a paid verification subscription to continue billing while the underlying account is locked?** If the service is not being delivered, is that a product — or a contract breach?
5. **What does an ICANN-accredited registrar's "good standing" mean** if an accredited registrar can weaponize a third-party platform's abuse channels to silence the researcher documenting their abuse-response failure? This is a compliance question, and it is being added to the existing RAA § 3.18 filing.

If Any Answer Was "No, This Is Not Fair"

Here are three concrete, zero-cost things, in ascending order of impact.

1. Share it publicly

Quiet disapproval does nothing. Visible pressure does. One click, pre-filled:

2. Ask the parties by name

Tag them. Silent disapproval does nothing. Visible questions from readers get noticed.

- **@NameSilo** — is the `@Phish_Destroy` ban related to your public statement offering to help the `xmrwallet` operator get detections removed?
- **@X / @XSupport / @elonmusk** — Email #2 says "restored to full functionality." The account is locked. Which ruling is operative?
- **@ICANN** — does RAA § 3.18 cover registrar retaliation against researchers?
- **@Tucows** — is platform-abuse retaliation against researchers compatible with your OpenSRS reseller standards?

3. Move your domains (this is the one that hurts)

Companies respond to revenue loss, not tweets. Transfers take about fifteen minutes. Our registrar statistics page lists registrars with clean abuse-response records. Every moved domain is a renewal-number datapoint NameSilo's leadership will see next quarter.

If you are an organization — crypto project, bug-bounty platform, journalism outlet, threat-intel company — with *any* domain at NameSilo: consider what it means to fund the registrar that sheltered a $20M+ theft operation and then silenced the researcher who documented it. You can make that move publicly. It carries weight.

Final Word

You don't get to protect a $20M+ theft operation for ten years, lie in public, and then silently stamp the researcher who caught you.

> You don't get to protect a $20M+ theft operation for ten years, lie about it in public, retaliate against the researcher who caught you — and have the whole thing quietly forgotten. Especially not while EU law enforcement is working the case.

We are not asking you to take our word. Every factual claim above is linked, documented, timestamped, archived off-site, and reproducible. We are asking you to look at the evidence, answer the five questions for yourself, and act on your own answer. That is what fair looks like — a reader who reads the evidence and decides. It is also exactly the thing that silencing is designed to prevent.

PhishDestroy is independent threat intelligence. Zero payments, zero sponsorships, zero favors. We publish what we find. NameSilo had us banned for it.

Original investigation: phishdestroy.io/xmrwallet-namesilo-exposed
Medium investigation (primary source): phishdestroy.medium.com/xmrwallet-com-2953f35b8a79
Evidence repo: github.com/PhishDestroy
