PhishDestroy Research

CYBERSECURITY THREAT INTELLIGENCE & DOMAIN ABUSE INVESTIGATION

phishdestroy.io
phishdestroy@proton.me
github.com/phishdestroy
PGP: available on request

FORMAL COMPLIANCE COMPLAINT — REGISTRAR MISCONDUCT

March 17, 2026

ICANN Contractual Compliance
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536, United States

Via: https://www.icann.org/compliance/complaint
Copy to: compliance@icann.org

> **RE:** Formal complaint against **NameSilo, LLC** (IANA ID: 1479) for violation of the Registrar Accreditation Agreement (RAA) in connection with domain **xmrwallet.com** — fabrication of abuse response, aiding active fraud operation, obstruction of multi-registrar enforcement action.

Dear ICANN Compliance Team,

We are submitting this formal complaint in our capacity as cybersecurity researchers who have conducted an extensive technical investigation into the domain **xmrwallet.com**, a confirmed Monero cryptocurrency theft operation active since 2016. We believe it is our professional and ethical obligation to escalate this matter to ICANN, as the registrar of record — **NameSilo, LLC** — has not only failed to act on a well-documented abuse report, but has actively fabricated a defense for the domain operator and assisted in undermining security vendor classifications.

This complaint is supported by technical evidence, the operator's own email correspondence, and the independent enforcement actions of three other ICANN-accredited registrars who reviewed the same evidence and suspended the operator's domains.

1. Background: The xmrwallet.com Fraud Operation

xmrwallet.com is a web-based Monero wallet that presents itself as a privacy-focused open-source tool. Our investigation, conducted between February and March 2026, established through live network capture and source code analysis that the site performs two distinct theft mechanisms:

1. **Private View Key Exfiltration:** On every API request, the user's private Monero view key is transmitted to the server encoded as Base64 within a `session_key` parameter. This key is sent 40+ times per session across 8 PHP endpoints. The operator can monitor all wallet balances and incoming transactions in real time.
2. **Server-Side Transaction Hijacking:** When a user initiates a transaction, the client-built transaction is discarded (`raw_tx_and_hash.raw = 0`) and replaced by a server-constructed transaction that redirects funds to an address controlled by the operator. A custom theft marker (`type == 'swept'`), absent from the Monero protocol, is used to track stolen transactions.

The operation has been active since **August 29, 2016** (domain registration date). We have documented **15+ victims** with confirmed losses exceeding **$2M USD equivalent** in Monero (XMR). The operator is identified as **Nathalie Roy** (Canada), GitHub username: nathroy (ID: 39167759), email: royn5094@protonmail.com.

Full technical evidence is publicly available at:
https://phishdestroy.github.io/DO-NOT-USE-xmrwallet-com/

2. Three Registrars Suspended — NameSilo Refused

Following publication of our findings, the operator registered four escape domains across four different registrars to maintain operations in the event of takedown. We submitted identical evidence packages to all registrars. The results were as follows:

DOMAIN	REGISTRAR	IANA ID	ACTION TAKEN
xmrwallet.cc	PublicDomainRegistry (PDR Ltd.)	303	SUSPENDED
xmrwallet.biz	WebNic.cc	460	SUSPENDED
xmrwallet.net	NICENIC International	2225	DNS DEAD (abuse action)
xmrwallet.com	**NameSilo, LLC**	**1479**	**REFUSED TO ACT**

Three independent, ICANN-accredited registrars in three different jurisdictions reviewed the same evidence and independently concluded that enforcement action was warranted. **NameSilo was the sole exception.**

3. NameSilo's Response: Fabricated “Compromise” Narrative

On **March 4, 2026**, NameSilo's abuse team responded to our report with the following position:

- The site was "compromised" — i.e., hacked by an unauthorized third party
- The operator is "the victim" of this compromise
- Therefore, no enforcement action would be taken

NameSilo provided zero technical evidence for this claim. No forensic report. No server logs. No timeline of the alleged breach. No identification of the alleged third party. No explanation of how malicious code was maintained across multiple domains, servers, and a Tor hidden service simultaneously for years.

> **Critical:** The "compromise" narrative is contradicted by the operator's own email correspondence with our research team, written *before* NameSilo was contacted and before the "compromise" story existed.

4. The Operator's Own Emails Contradict NameSilo's Claims

Between **February 16 and February 23, 2026**, the xmrwallet.com operator emailed PhishDestroy directly from `royn5094@protonmail.com`. These communications occurred *before* we filed any abuse report with NameSilo. The operator's own words prove that no compromise occurred:

Email #1 — February 16, 2026

> *"We don't store seeds or keys, everything is done in your browser locally. Please remove your report. N.R."*
>
> From: royn5094@protonmail.com → PhishDestroy

Significance: First person ("we"). Defends the site as his own operation. No mention of any compromise or unauthorized access. Meanwhile, live network capture confirms `session_key = Base64(private_view_key)` transmitted to the server 40+ times per session.

Email #2 — February 17, 2026

> *"This is the data we need to offer the service."*
>
> From: royn5094@protonmail.com → PhishDestroy

Significance: Within 24 hours, the operator contradicts his own prior statement. Yesterday: "we don't store keys." Today: "this is the data we need." Still first person. Still no mention of any hack.

Email #3 — February 17, 2026

> *"Feel free to subpoena the domain registrar for my information to submit a complaint in the courts."*
>
> From: royn5094@protonmail.com → PhishDestroy

This statement is the most significant piece of evidence in this complaint. It was written on February 17 — before we contacted NameSilo, before any abuse report was filed, and before the "compromise" story existed. An operator running $550/month bulletproof hosting behind DDoS-Guard (specifically to resist takedowns) does not casually invite registrar scrutiny — unless he already knows the registrar will protect him. He did not say "subpoena the hosting provider." He specifically said "subpoena *the registrar*" — NameSilo — with complete confidence.

Email #4 — February 23, 2026

> *"I've hired a lawyer and a private investigator."*
> *"Trezor and Ledger also get their view keys."*
>
> From: royn5094@protonmail.com → PhishDestroy

Significance: Sent the same day xmrwallet.cc and xmrwallet.biz were suspended. The lawyer never materialized. The claim that "Trezor and Ledger also get view keys" is technically illiterate — Trezor is a hardware wallet with no server component. Still no mention of any compromise. Still defends the code as his own.

5. Timeline: The "Compromise" Story Was Fabricated After the Fact

DATE	EVENT	WHO MENTIONED "HACK"?
Feb 16	Operator emails: "We don't store keys"	Nobody
Feb 17	Operator emails: "This is the data we need"	Nobody
Feb 17	Operator emails: "Subpoena the registrar"	Nobody
Feb 23	Operator emails: "I've hired a lawyer"	Nobody
Feb 23	xmrwallet.cc and .biz SUSPENDED	Nobody
Mar 4	**NameSilo responds to abuse report**	**NameSilo**

The operator communicated with us four times. In every communication, he used first person, defended the code as his own creation, and never once referenced any hack, compromise, or unauthorized third-party access. **The "compromise" narrative appeared for the first time on March 4 — in NameSilo's response.** Not from the operator. From NameSilo.

6. Additional Misconduct: VirusTotal Flag Removal

At the time of our investigation, xmrwallet.com was flagged as malicious by multiple security vendors on VirusTotal, including **Fortinet** (Phishing), **ESET**, **Sophos**, and others. Following NameSilo's involvement, the operator initiated removal of these security classifications. NameSilo's "compromise" narrative was used as justification to request delisting from threat intelligence databases.

This constitutes active assistance in undermining the cybersecurity ecosystem's ability to protect users from a confirmed fraud operation.

7. Specific RAA Violations

We believe NameSilo's conduct violates the following provisions of the 2013 Registrar Accreditation Agreement:

1. **Section 3.18 — Abuse Contact and Abuse Handling:** NameSilo is required to "take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse." Fabricating an exculpatory narrative without evidence and in contradiction to the operator's own statements does not constitute an appropriate response.

2. **Section 3.18.1 — Abuse Point of Contact:** NameSilo's abuse team functioned not as a neutral compliance body but as an advocate for the reported party, actively constructing a defense rather than investigating the report.
3. **Section 3.7.7 — WHOIS Accuracy:** The operator maintains WHOIS privacy while conducting documented fraud. NameSilo's refusal to act on the domain preserves this protection for an active theft operation.
4. **ICANN Consensus Policy — DNS Abuse:** Phishing and fraud constitute DNS abuse under ICANN's framework. NameSilo's response does not meet the standard of reasonable investigation expected of an accredited registrar.

8. Evidentiary Record

The following evidence is publicly available and verifiable:

EVIDENCE	LOCATION
Full technical investigation (code analysis, network captures)	https://phishdestroy.github.io/DO-NOT-USE-xmrwallet-com/
NameSilo cover-up analysis with operator email evidence	https://phishdestroy.github.io/DO-NOT-USE-xmrwallet-com/posts/post-namesilo-xmrwallet-coverup.html
Archived deleted GitHub issues #35 and #36	https://phishdestroy.github.io/DO-NOT-USE-xmrwallet-com/deleted.html
VirusTotal classification (multiple vendors)	https://www.virustotal.com/gui/domain/www.xmrwallet.com
Medium article with full analysis	https://phishdestroy.medium.com/xmrwallet-com-2953f35b8a79
GitHub repository with all evidence archived	https://github.com/phishdestroy/DO-NOT-USE-xmrwallet-com
Operator email screenshots (4 emails, Feb 16–23)	Available in the NameSilo cover-up analysis page above

Operator email correspondence originals are preserved and can be provided to ICANN upon request with full headers for authentication.

9. Requested Actions

We respectfully request that ICANN Contractual Compliance:

1. **Investigate NameSilo's handling of abuse report** regarding xmrwallet.com, including the basis for their "compromise" determination and whether any technical evidence was produced.
2. **Determine whether NameSilo's abuse team has a conflict of interest** or undisclosed relationship with the operator of xmrwallet.com, given the operator's foreknowledge that NameSilo would not act ("subpoena the registrar").
3. **Review NameSilo's compliance with RAA Section 3.18** regarding their obligation to investigate and respond appropriately to abuse reports.
4. **Consider enforcement action** including formal notice of breach, remediation requirements, or referral for further investigation.
5. **Suspend or place serverHold on xmrwallet.com** pending investigation, consistent with the actions taken by three other accredited registrars on the operator's other domains.

10. Conclusion

As cybersecurity professionals, we consider it our duty to escalate this matter. The evidence is unambiguous: the operator built this theft infrastructure, maintains it across multiple domains and a Tor hidden service, and has been stealing cryptocurrency from users since 2016. Three ICANN-accredited registrars independently confirmed this assessment. NameSilo not only failed to act but actively constructed a false narrative to protect the operator.

We do not make this complaint lightly. We have exhausted all available channels with NameSilo directly. Their abuse team's response was not negligent — it was deliberately protective of a confirmed fraud operation. The operator's own words, written before NameSilo's involvement, prove that the "compromise" story is a fabrication.

We are available for further discussion, evidence submission, or technical briefing at ICANN's convenience.

Respectfully submitted,

PhishDestroy Research

Cybersecurity Threat Intelligence & Domain Abuse Investigation

Web: https://phishdestroy.io
Email: phishdestroy@proton.me
GitHub: https://github.com/phishdestroy
Twitter/X: @Phish_Destroy
Telegram: @destroy_phish