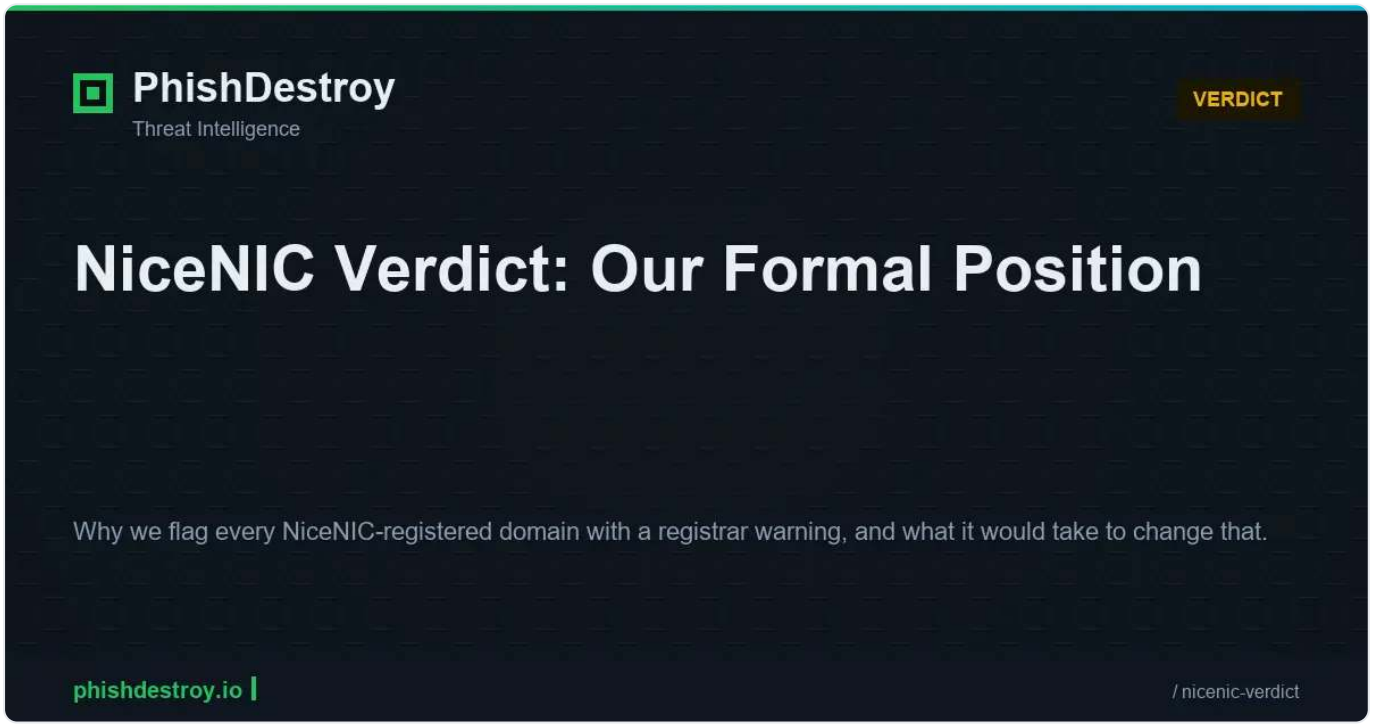
THREAT INTELLIGENCE REPORT

NiceNIC Verdict: Every Domain Reviewed, Zero Legitimate Uses Found

Ref. **PD-TI-2026-66199** Published **10 July 2026** Source **phishdestroy.io/nicenic-verdict**

Follow-up Investigation
IANA 3765 · NICENIC INTERNATIONAL GROUP CO., LIMITED · Hong Kong

9 min read · Updated **March 2026** · PhishDestroy Intelligence



5,000+
Unique Tickets Ignored
24.7 MB
Domain Dataset Published
0
Legitimate Domains Found
100%
Domains Now Flagged

We Decided to Check

After our first investigation exposed NiceNIC as the ICANN-accredited registrar powering global cybercrime, one question remained: is it really ALL bad? Could there be legitimate businesses buried under the mountain of phishing, crypto scams, and worse?

We decided to find out. We reviewed NiceNIC's entire domain portfolio — every registration, every IP, every piece of content we could access. The result is a 24.7 MB dataset published on GitHub for anyone to verify independently.

The conclusion was unanimous and unambiguous.

The Result

We looked for ANY legitimate use case. A single clean business. A personal blog. A portfolio site. **We found none.**

This investigation builds on our original findings. Read the full context:

- Our first NiceNIC investigation (August 2025)
- DecodeCybercrime independent investigation

What We Found

The domains registered through NiceNIC fall into clear categories of abuse:

Category	Prevalence	Notes
Crypto Phishing & Drainers	**Dominant**	Wallet drainers, fake exchanges, airdrop scams
Fake Gambling & Casinos	**High**	Linked to operations we've already investigated (OFEDREX, LuxardGambling)
Phishing (General)	**High**	Credential harvesting, brand impersonation
Malware Distribution	**Moderate**	Drive-by downloads, fake software
Undisclosed Criminal Content	**Present**	Content violating criminal law in every jurisdiction — deliberately not described

Content Warning

Some content hosted on NiceNIC domains is so extreme that describing it in detail would itself be irresponsible. There are categories present that violate criminal codes universally. **We documented everything. We will not publish specifics.**

The only "borderline" category was gambling — but even that fell apart under scrutiny. The gambling domains traced directly back to fake casino operations we had already investigated: **OFEDREX** with its 383 verified victims, **LuxardGambling** with its deepfake celebrity endorsements. These aren't legitimate gambling sites. They're the same scam panels wearing different skins.

The Hacker Forum Connection

NiceNIC's relationship with cybercriminals goes far beyond passive negligence. The registrar actively participates in the ecosystem:

"NiceNIC maintains an active presence on BlackHatWorld, a forum notorious for SEO spam, phishing toolkits, and fraud services."
"Promotional emails from NiceNIC have been documented boasting 'fewer abuse reports' — marketing copy designed specifically to attract criminal customers."

"When abuse is reported, NiceNIC forwards the reporter's personal contact information — including email addresses — directly to the domain owner. This isn't an oversight. It's a feature designed to intimidate whistleblowers."

Key Incidents

Infographic: 5,000 abuse reports sent to NiceNIC, 0 actions taken — mountain of ignored reports in trash

BreachForums Incident

NiceNIC unsuspended a domain **AFTER an FBI takedown request** , then reportedly suspended the FBI's own account to prevent further correspondence.

Telegram @NiceNIC_NET

Documented conversations discussing **disabling WHOIS** and providing bulletproof services to suspected criminals.

GDPR / Privacy Violations

Sharing reporter data with attackers — turning the abuse reporting process into a weapon against whistleblowers.

5,000 Tickets Ignored

The number is not an estimate. It is not inflated with duplicates. **5,000+ unique abuse tickets** were filed against NiceNIC domains — each with fresh evidence, each for a different malicious domain. This count excludes repeat escalations, follow-up submissions, and cross-referenced reports.

The response pattern was always the same:

"Insufficient evidence" — NiceNIC's standard auto-reply to forensic PDFs containing VirusTotal reports with 15+ vendor detections, full page screenshots of active phishing portals, DNS mapping, and

technical metadata.

Mechanisms of Abuse

- **48-hour suspension delay:** NiceNIC's internal policy allows reported domains to remain active for 48 hours, giving scammers ample time to drain victims
- **WHOIS/RDAP manipulation:** intentionally broken or disabled for clients upon request, violating ICANN RAA transparency requirements
- **Auto-closed complaints:** tickets sent to abuse@nicenic.net are automatically forwarded to domain owners and closed

The Business Decision

5,000 tickets is not a compliance failure. It is a business decision. **Every ignored ticket is revenue protected.**

Our Verdict

Based on the evidence — the complete domain review, the 5,000+ ignored tickets, the hacker forum presence, the FBI incident, the whistleblower intimidation, and the confirmed zero legitimate use rate — PhishDestroy has made a definitive decision:

Official Designation

Every domain registered through NiceNIC (IANA 3765) is now flagged as potentially unsafe in PhishDestroy's threat intelligence system. This applies to our API, blocklists, browser warnings, and all partner integrations.

This is not a blanket punishment. It is a statistical conclusion. When 100% of reviewed content is malicious and the registrar actively enables it, the registrar IS the criminal infrastructure.

Final Statement

This is not negligence. This is not incompetence. This is a business model built on abuse resilience. **The owners of NICENIC INTERNATIONAL GROUP CO., LIMITED should face criminal liability** — not for failing to act, but for deliberately choosing not to. We are waiting for accountability.

The business model is clear: charge criminals for domains, ignore all abuse reports, share whistleblower data with attackers, advertise on hacker forums. This is not a grey area. This is organized infrastructure for organized crime. A legal precedent here would send a message to every bulletproof registrar operating under ICANN's umbrella.

Play the Game: Find a Legitimate Domain

We're making the challenge public. The complete dataset is published. Every NiceNIC domain we reviewed is available for download and independent verification.

The rules are simple: find a single legitimate domain registered through NiceNIC. A real business. A personal website. Anything that isn't phishing, scamming, or worse.

If you find one, tell us. We haven't.

trash.json (24.7 MB)

Complete NiceNIC domain collection with registration dates, IPs, and registrar data. Download and verify independently.

DestroyList Repository

Open-source blocklist of 80,000+ phishing domains. Real-time updates, community contributions.

Interactive Tools

Free API, threat scoring, bulk checking. No API key required.

Threat Intelligence API

Check any domain instantly. Risk scoring 0-100, bulk analysis up to 500 domains per request.

Our First Investigation

NiceNIC Exposed: phishing score 1,141.74, $8.5M Trust Wallet heist link, ICANN complicity.

DecodeCybercrime Investigation

Independent confirmation: NiceNIC as the leading bulletproof registrar enabling global cybercrime.

Further Reading & References

- PhishDestroy on Medium: NiceNIC Exposed
- DecodeCybercrime: NiceNIC — The Leading Bulletproof Domain Registrar
- Trustpilot: NiceNIC user reviews on abuse handling and phishing domains
- NiceNIC.support: Abuse reporting process and ICANN compliance issues
- DEV.to: The Backbone of Global Scam — NameSilo, WebNIC, and NiceNIC
- CyberCrime InfoCenter: Registrar phishing domain ranking (includes NiceNIC)
- Interisle: Phishing Trends — registrars with high phishing domain counts

#NiceNIC #ICANN #RegistrarVerdict #Investigation #CyberCrime
