THREAT INTELLIGENCE REPORT

NiceNIC Exposed: The ICANN Registrar Powering Global Cybercrime

Ref. **PD-TI-2026-45952** Published **10 July 2026** Source **phishdestroy.io/nicenic-real**

IANA 3765 Investigation

Investigation into an ICANN-accredited registrar with unprecedented phishing score of 1,141.74 — providing structural sanctuary for scam networks, facilitating the $8.5M Trust Wallet heist, and openly admitting "we are not against scamming."

8 min read · Updated **March 2026** · PhishDestroy Intelligence
Phishing Score: 1,141.74 Trust Wallet Heist: $8.5M IANA ID: 3765

0
Phishing Score
320x
More Fraud Than Norm
0
Soulless Machine Sites

$8.5M
Trust Wallet Loss

The Statistical Impossibility

NiceNIC is not just a "poor performer" — it is a statistical impossibility in legitimate commerce. According to the Cybercrime Information Center's 2025 data, their phishing score of **1,141.74** makes them host *320 times more confirmed fraud per registration* than industry norms.

Phishing Score Comparison (2025)

3.5
GoDaddy
3.2
Google
8.4
Reg.ru
1,141
NiceNIC

What This Means

While legitimate registrars maintain scores below 10, NiceNIC operates at **100-300x the industry average** . This is not negligence — this is infrastructure designed for fraud. These indicators of compromise (IOCs) demonstrate systematic abuse-tolerant hosting practices that violate ICANN compliance standards.

The "Insufficient Evidence" Tactic

PhishDestroy sends comprehensive forensic packets to NiceNIC containing:

- **Forensic PDFs** with malicious script signatures & drainer code
- **VirusTotal reports** showing 15-20+ vendor detections
- **Screenshots** of fraudulent login portals
- **DNS history** and IP mapping
- **JSON metadata** with technical indicators

Their automated response claims this is not enough:

"Thank you for submitting your report... However at this stage the information provided is not sufficient for our team to verify the issue..."

— NiceNIC Compliance Team (auto-reply)

The Truth

Evidence confirms NiceNIC support staff **deliberately refuses to open attachments** to maintain legal "deniability." Domains reported with 16+ VirusTotal detections remain active for 1,000+ hours. This pattern undermines domain threat intelligence efforts across the industry.

Recommended By Scammers

Dark web forum post recommending NiceNIC because they ignore all abuse reports - EXPOSED

Research by **Brian Krebs** ("Soulless" investigation) exposed NiceNIC as the primary home for Russian *Gambler Panel* networks. Scam-panel operators actively train their affiliates to use NiceNIC.

"Use NiceNIC. They are loyal to our business. If PhishDestroy reports, ignore it. NiceNIC will send their standard 'lack of evidence' refusal automatically."

— Leaked Telegram instructions from Gambler Panel operators

Soulless Machine

Brian Krebs identified a network of over **1,200 identical scam sites** using NiceNIC infrastructure — all running the same drainer scripts.

Gambler Tech Intel

Telegram groups openly recommend NiceNIC for hosting crypto drainer operations, citing their "loyalty to business."

The $8.5M Trust Wallet Heist

December 2025 — NiceNIC's most catastrophic failure

$8,500,000
Confirmed Loss Threshold

Full Stack Control

NiceNIC was both the **Registrar AND Host** for the exfiltration infrastructure. They had absolute technical power to kill the nodes but deliberately kept them online.

Operator Watching Live

The NiceNIC operator was **Online in Telegram** during the heist. They lacked Premium privacy, exposing their status. They ignored forensic alerts as millions were stolen.

100% Operational Continuity

Infrastructure remained active until the final cent was drained. NiceNIC provided the thieves with complete operational support.

Exfiltration Infrastructure

NS3.MY-NDNS.COM
NS4.MY-NDNS.COM

The Public Confession

On January 10, 2026, NiceNIC's Twitter account posted a manifesto that shocked the security community:

"We are not against scamming... we here to make cash."
After the post went viral, they staged a fake "Russian hack" using the name **"Juliani"** to maintain deniability before ICANN. But the damage was done — their true stance was revealed.

The Pattern Is Clear

Automated refusals + scammer endorsements + Twitter confession + $8.5M heist = This is not a compliance failure. This is a business model.

Evidence & Documentation

Download the forensic reports that NiceNIC claims are "insufficient":

Escalation #17: bigspin.cc

1398 hours online • 16/95 VirusTotal • Soulless Engine signatures

Initial Report: caivax.com

Crimes Ordinance Cap.200 • IP: 104.21.23.244 • SENT & IGNORED

Live Threat Map

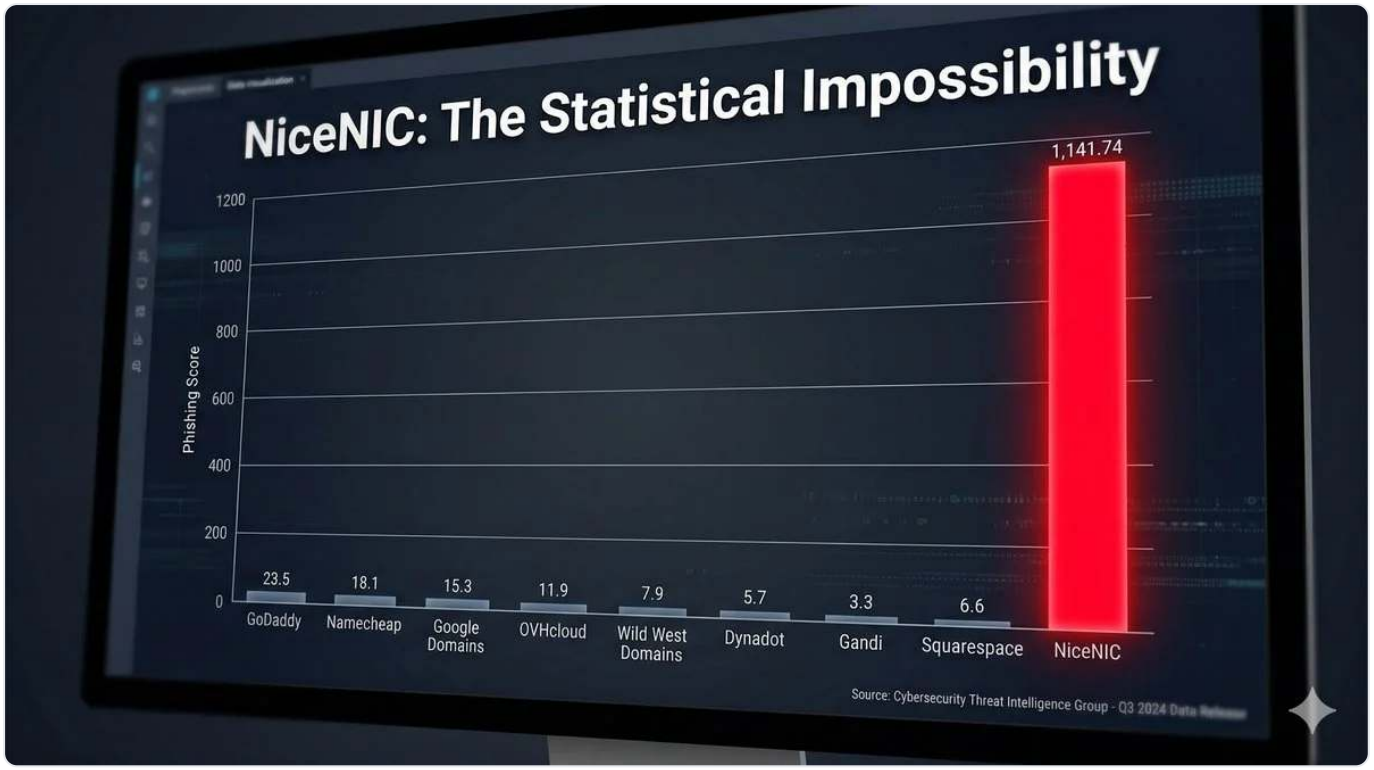
Real-time tracking of active drainers and phishing nodes

Gambler Tech Intel

Source: Scammer training materials recommending NiceNIC

#NiceNIC #ICANN #RegistrarAbuse #Investigation #DomainAbuse

Related Research



NiceNIC vs other registrars — phishing density score comparison

Registrars Enabling Global Scams

How ICANN registrars NameSilo, Webnic, and NiceNic keep scam infrastructure alive by ignoring abuse.

Gambler Panel: Crime Network Analysis

Deep dive into organized crime infrastructure operating 1,200+ fraudulent casino domains.

Scam Intelligence Dashboard

Exposing crypto scammer infrastructure, collecting evidence, and helping victims fight back.
