⚠ ESCALATION REPORT

Unresolved Phishing Threat

FOLLOW-UP #17 • 1398H ACTIVE

REPORT DATE	CASE REFERENCE	REPORT NUMBER	PRIORITY
January 12, 2026	#PD-1768240314-bigspin.cc	#17 (Escalated)	CRITICAL

⚠ Escalation Status — Immediate Action Required

1398	17	16
HOURS ACTIVE	REPORTS SENT	NO RESPONSE

⚠ **This domain continues to victimize users while previous reports remain unaddressed.**
If you are unable to take action, please escalate this report to your **Abuse Department Manager** or **Trust & Safety Lead** immediately. Documented non-response may be included in ICANN compliance reports and public transparency disclosures.

To the NICENIC INTERNATIONAL GROUP CO., LIMITED Abuse & Security Team,

This is **follow-up report #17** regarding confirmed phishing activity on the domain listed below. Despite 16 previous notification(s) over 1398 hours, this malicious site remains operational and continues to defraud users.

ESCALATED — 17 REPORTS WITHOUT ACTION

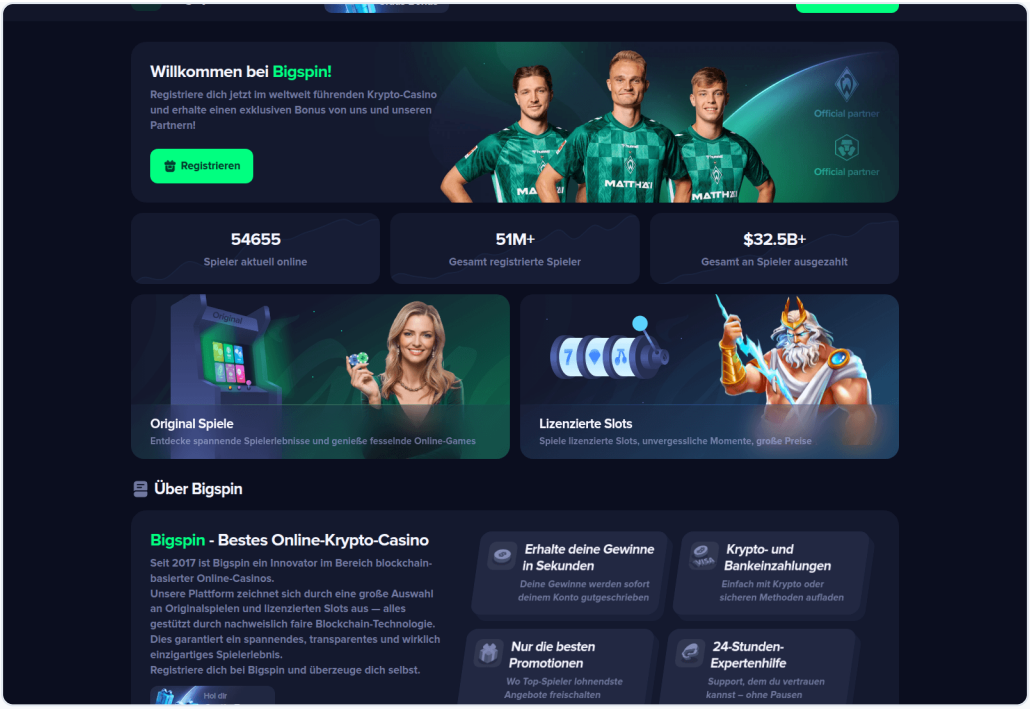
Technical Evidence

MALICIOUS DOMAIN	`bigspin.cc`
TARGET BRAND	Web3/Crypto
RESOLVED IP	`188.114.97.3`
DETECTION TIME	2026-01-12 17:52:12 UTC
URLSCAN REPORT	View Full Analysis →

Multi-Vendor Threat Intelligence

VIRUSTOTAL	**16/95** malicious detections alphaMountain.ai, BitDefender, CRDF, CyRadar, ESET View full report →
BLACKLIST STATUS	**SEAL**

VISUAL EVIDENCE (AUTOMATED SCREENSHOT)



THREAT ANALYSIS SUMMARY

The domain bigspin.cc has been active for 1398 hours and poses a confirmed threat based on multiple independent sources. VirusTotal detected 16 out of 95 vendors, including notable names like BitDefender and ESET, flagging it as malicious. Additionally, it is listed on SEAL's blacklist, further corroborating its fraudulent activities. According to NICENIC International Group's policy, the use of services for unlawful purposes is strictly prohibited, with violations potentially leading to immediate suspension. The ongoing phishing activities associated with this domain not only contravene your policies but also expose your organization to legal liability under the Crimes Ordinance and the Personal Data (Privacy) Ordinance. Immediate action is warranted to prevent further victim harm and mitigate risk.

⚖ Legal & Policy Violations

The domain bigspin.cc has been active for 1398 hours and poses a confirmed threat based on multiple independent sources. VirusTotal detected 16 out of 95 vendors, including notable names like BitDefender and ESET, flagging it as malicious. Additionally, it is listed on SEAL's blacklist, further corroborating its fraudulent activities. According to NICENIC International Group's policy, the use of services for unlawful purposes is strictly prohibited, with violations potentially leading to immediate suspension. The ongoing phishing activities associated

with this domain not only contravene your policies but also expose your organization to legal liability under the Crimes Ordinance and the Personal Data (Privacy) Ordinance. Immediate action is warranted to prevent further victim harm and mitigate risk.

⚠ Non-Response Documentation

This domain has been reported **17 times** over **1398 hours** without visible action. This pattern of non-response is being documented and may be included in:

- → ICANN Registrar Compliance complaints
- → Public transparency reports on registrar abuse handling
- → Law enforcement referrals and evidence packages

Social Engineering Warning for Abuse Staff

Phishing operators actively train to manipulate registrar support staff. They use prepared scripts and professional language to appear legitimate. Common tactics include:

- → **"False positive"** — claiming PhishDestroy or security vendors made an error
- → **"Competitor attack"** — alleging the report is sabotage from business rivals
- → **"Verification needed"** — requesting delays while they drain more victims
- → **"Legitimate business"** — providing fake documentation or incorporation papers
- → **"Legal threats"** — threatening lawsuits against the registrar for suspension
- → **"Already fixed"** — claiming the issue was resolved (while keeping drainer active)

⚠ **Do not engage in prolonged correspondence.** Multi-vendor detections from VirusTotal, URLQuery, and public blacklists are not mistakes. Every hour of "investigation" or "verification" means more victims losing funds. When in doubt, suspend first and allow the registrant to appeal with verified documentation.

✓ Required Remediation Actions

- → **Immediate Suspension:** Disable DNS resolution for the reported domain

- → **Account Audit:** Review registrant for additional malicious domains
- → **Evidence Preservation:** Retain WHOIS and access logs for law enforcement
- → **Internal Escalation:** Forward to Abuse Manager — this is report #17

REPORT TIMELINE

2025-11-15 11:49:06 UTC
Initial report submitted

2026-01-12 17:52:12 UTC
Current: Escalation Report #17 — Domain still active after 1398h

> **Transparency & Compliance:** This report has been documented in the **PhishDestroy Destroylist** public database. Per **ICANN RAA §3.18**, registrars must investigate and respond to abuse reports expeditiously.

Respectfully,

PhishDestroy

PhishDestroy.io Security Team
phishdestroy.io • X/Twitter • Telegram