FINTELEGRAM COMPLIANCE INTELLIGENCE REPORT

Cyberfinance Intelligence

Zentoria / Spinsopotamia and the NALMI Casino Network

A Consolidated Brand, Infrastructure and Byte-Identical Asset Correlation Analysis

Contents

Content

1. Executive Summary

This report consolidates four completed public-source collection packages and the prior Zentoria technical and corporate evidence sets into a single correlation model. It is written for regulators, payment-institution compliance teams, acquiring banks, wallet providers, crypto exchanges, legal counsel and investigative journalists. Its purpose is to set out, layer by layer, what the combined public evidence does and does not establish about the relationship between a Zentoria-facing casino anchor and a large, concentrated population of casino-related domains.

The central public anchor is the domain **SPINSOPOTAMIA.COM**. In earlier FinTelegram reporting this domain was identified as the publicly visible billing descriptor and casino entry point associated with **Zentoria Limited**, an Irish-registered entity holding a Remote Bookmaker's Licence. According to that prior reporting, the descriptor “Spinsopotamia.com Dublin” has appeared on the card statements of players who deposited into offshore casino brands within the NovaForge group, positioning the domain as a clean, EU-facing payment facade in front of higher-risk brands. The present report treats Spinsopotamia.com as a public-facing wrapper and entry point, not as proof of ownership of any downstream brand.

The key infrastructure observation is **concentration, not exact-IP identity**. Of 496 investigated casino-related domains, 495 resolve inside the single routed prefix **185.207.196.0/22**, under the **NALMI / AS213846** infrastructure envelope. The Zentoria-facing endpoint Spinsopotamia.com currently resolves to **185.207.197.216**, a host address that differs from the 491-domain majority sitting in the 185.207.196.0/24 sub-range, but which lies inside the same /22 prefix, the same ASN and the same provider layer. The exact host differs; the prefix, ASN and provider converge.

Beyond infrastructure, the combined dataset exposes multiple, reproducible technical correlation layers. At the application layer, after generic provider-managed files were removed, 120 meaningful byte-identical asset groups connect 98 domains into 16 technical components spanning 29 observed brand families. At the telemetry layer, 51 domains across 14 brand families expose identical Sentry Replay sampling values. At the platform and service layer, recurring components — including an explicit SPTPub platform host, plus widely repeated analytics, fraud-intelligence, support and payment integrations — point to a templated, centralised casino-platform environment. Each layer is established independently and is not silently converted into a match at any other layer.

Technical finding — HIGH correlation value

The combined dataset establishes a highly concentrated casino-domain infrastructure environment, a direct infrastructure bridge from the Zentoria-facing Spinsopotamia.com endpoint into that same NALMI /22 envelope, and multiple reproducible byte-identical deployment families. It does **not** establish that Zentoria Limited legally owns or operates every observed domain, that a single ultimate beneficial owner sits behind all 496 domains, or that any criminal or regulatory liability exists as a matter of law. Provider, tenant, payment and contracting records remain decisive.

In short, the report converts a large body of public-source observation into a compact, well-defined target area. It identifies specific disclosure targets — infrastructure provider, edge/CDN provider, platform, telemetry, support and payment providers — that hold the account-level records needed to move from technical correlation to any legal attribution. It does not pre-empt those records, and it does not assert conclusions that only provider-level evidence and a competent regulator can reach.

2. Background: Zentoria, Spinsopotamia and NovaForge

This section summarises the framing established in prior FinTelegram reporting. It is provided as narrative context only. Statements attributed to FinTelegram's earlier coverage or to named regulators are reproduced as allegations, whistleblower attributions or regulator findings of those sources, and are not independently re-established by the technical dataset that forms the core of this report.

2.1 Zentoria Limited as a payment-facing entity

FinTelegram has presented **Zentoria Limited** as an Irish-registered company (CRO 761150, incorporated 4 April 2024, registered in Dublin 4) holding a Remote Bookmaker's Licence from the Irish Revenue Commissioners, with gambling and betting activities as its principal listed activity. In that reporting, the named individuals associated with the company are described as **Mykhaylo Pavlenko** and **Alina Vavilova**. These are corporate-registry and prior-reporting details; the present report does not make any independent finding about these persons, who are entitled to the presumption of innocence and to a right of reply.

Prior coverage frames Zentoria as a “Trojan Horse” payment layer: an EU-anchored, licensed merchant identity used, according to whistleblower and victim accounts cited by FinTelegram, to present card transactions under the benign descriptor ***“Spinsopotamia.com Dublin”*** rather than under the names of offshore casino brands. This report restates that framing as an allegation of those sources and does not itself adjudicate whether transaction-laundering occurred.

2.2 The significance of Spinsopotamia.com

The domain **Spinsopotamia.com** matters in earlier coverage for three reasons. First, it is the human-readable billing descriptor reported on player card statements. Second, it is described as a live website serving as a legitimate-looking front, providing cover for deposits routed to offshore brands such as Robycasino and Spinsy within the NovaForge group. Third, a subsequent FinTelegram update reported a whistleblower attribution connecting the “Spinsopotamia.com” descriptor to **xpate** (xpate.com), a payment-services / e-money firm that states it is authorised by the UK Financial Conduct Authority as an Electronic Money Institution. That attribution is a whistleblower-sourced lead in the prior reporting and would require provider-level confirmation before any conclusion could be drawn.

Later FinTelegram reporting also examined whether several casino brands are linked through a shared cashier and payment-rail stack, citing a live test deposit into Spinsy whose transaction detail surfaced “Zentoria Limited” as payee, alongside other payee descriptors and a recurring open-banking deposit path. That reporting expressly stops short of asserting that Zentoria owns every brand in the cluster, instead supporting the narrower conclusion that the brands likely sit on a shared backend orchestration environment. The present technical report is consistent with that cautious framing.

2.3 NovaForge and the wider casino ecosystem

In prior reporting, **NovaForge** is presented as the operator group or hub behind a set of offshore casino brands (including Robycasino and the ACMA-blacklisted Spinsy) that rely on EU/UK-facing payment facades to reach mainstream card and banking rails. A related FinTelegram analysis introduced **NALMI** as a possible infrastructure envelope behind a large, rotating casino-domain ecosystem, and noted that this technical ecosystem intersects with domains and public-facing wrappers already relevant to the Zentoria line of research.

2.4 Why Spinsopotamia and Zentoria came under scrutiny

Public scrutiny of Spinsopotamia.com and Zentoria arose, according to those sources, from a convergence of signals: player complaints and victim card statements showing an unexpected EU descriptor for deposits into offshore brands; the contrast between an active EU bookmaker licence and the offshore status of the brands actually being funded; whistleblower documentation pointing to specific payment nodes; and brand-and-rail overlaps suggesting a shared backend. The technical dataset analysed below was assembled to test, on public evidence alone, whether and how the Zentoria-facing anchor connects to the wider casino-domain population at the infrastructure, application, telemetry and platform layers.

3. Methodology and Evidence Boundary

The technical findings in this report derive from a four-virtual-machine ("four-VM") public-source collection exercise and a set of separately documented prior evidence packages. The methodology is summarised here in the report's own words; the underlying packages retain the raw artefacts, worker logs, stage results and cryptographic manifests.

3.1 Public sources only

Collection used public sources exclusively: current DNS records and apex A-records, certificate-transparency logs, publicly accessible URLScan references, and publicly served HTML and JavaScript assets. No login was performed, no account was created, no deposit or payment flow was initiated, no authentication endpoint was tested, and no access-control or anti-bot mechanism was bypassed. The exercise observed only what any member of the public could observe from outside the casino platforms.

3.2 Collection scale and integrity

Metric	Result
Unique investigated domains	496
Manifest-verified files	3,060 / 3,060
Manifest mismatches	0
Apex A-record rows	838
Distinct IPv4 addresses	142
Certificate-transparency rows	30,189
URLScan references	959
Retained HTML / JavaScript artefacts	1,181
Meaningful cross-domain hash groups	120

Manifest verification matched all 3,060 collected files against their recorded SHA-256 values with zero mismatches, establishing that the analysed artefacts are the artefacts that were collected.

3.3 Evidence cleaning

Generic Cloudflare challenge files, provider-managed anti-bot assets and other non-attributive third-party files were removed from primary correlation, because their presence reflects shared infrastructure usage rather than any application-specific relationship. The consolidated review retained 120 first-party / application hash groups for correlation, excluded 26 generic Cloudflare groups, and treated six third-party groups as supporting context only.

3.4 Evidence weighting system

Each claim is graded by how the underlying observation was established, not by the seriousness of any inference that might be drawn from it. Four tiers are used throughout this report:

Tier	Definition
PRIMARY	Direct DNS records, current IP assignments, ASN / provider data, direct public hostnames, byte-identical SHA-256 application assets, or preserved raw network evidence.
SECONDARY	A finding corroborated by two or more independent non-primary sources.

Tier	Definition
LEAD	A single public indicator that requires further verification before any weight is placed on it.
BACKGROUND	Generic provider context (for example, Cloudflare as an edge / CDN layer) that does not support ownership attribution by itself.

Shared hosting, common CDN use and common advertising networks are not treated as ownership evidence. Application-specific byte identity, direct platform hostnames and stable account identifiers carry materially greater weight. A match at one layer — domain, endpoint, prefix, ASN, application asset, telemetry or platform integration — is never silently converted into a match at every other layer.

3.5 The no-negative-inference rule

No-negative-inference rule

Blocked HTTP fetches, missing URLScan detail responses, certificate-transparency timeouts, or the absence of a saved JavaScript artefact are recorded as incomplete collection. They are not interpreted as proof that a marker or relationship is absent. In particular, Spinsopotamia.com produced no meaningful shared-asset hash in the current four-VM run because its public artefact collection was incomplete; the network correlation for that domain is established independently by DNS and prefix data, and the missing asset match must not be treated as disproof.

4. Infrastructure Concentration: NALMI /22 and the Casino Domain Environment

The prior Zentoria evidence set identifies Spinsopotamia.com as the key public-facing entry point associated with Zentoria Limited. The four-VM DNS evidence independently records the same domain resolving to **185.207.197.216**. This section sets out the infrastructure bridge from that endpoint into the wider casino-domain population, and draws an explicit boundary around what the bridge does and does not prove. **[PRIMARY]**

4.1 The infrastructure bridge

The relationship can be read as a four-stage chain: a legal / public anchor (Zentoria Limited, presented publicly through Spinsopotamia.com); a current network endpoint (185.207.197.216, served behind a Cloudflare edge); a network envelope (185.207.196.0/22, AS213846, NALMI Limited); and the wider dataset (496 investigated casino-related domains, of which 98 are linked into application components). The exact IP of the anchor differs from most 185.207.196.x endpoints, but the /22 prefix, the ASN and the provider layer are the same.

> **Identical network layer**
>
> **185.207.196.0/22 | AS213846 / NALMI LIMITED**

4.2 Exact IP and prefix comparison

Comparison point	Zentoria / Spinsopotamia	Wider four-VM dataset	Assessment
Public anchor	SPINSOPOTAMIA.COM	496 investigated casino-related domains	Anchor relationship derives from the prior Zentoria evidence set.
Current endpoint	185.207.197.216	142 distinct IPv4 addresses	Different exact host from most domains, but inside the same wider routed environment.
Immediate /24	185.207.197.0/24	491 in .196/24; 2 in .197/24; 1 in .198/24; 1 in .199/24	Same /22 environment; only partial /24 overlap.
Aggregate prefix	**185.207.196.0/22**	**495 of 496 domains**	**IDENTICAL — exact prefix match at /22 level.**
Origin / provider	**AS213846 / NALMI LIMITED**	**Same for the 495-domain /22 population**	**IDENTICAL — same provider and routed layer.**
Edge / delivery	Cloudflare observed in prior active-routing and header evidence	Cloudflare widely observed across the four-VM URLScan corpus	Common edge class; not proof of common ownership.
Application hash match	None retained in current run	120 meaningful groups across 98 domains	Collection gap; no negative inference.

4.3 The /22 envelope

The range 185.207.196.0/22 spans 185.207.196.0 through 185.207.199.255 — 1,024 IPv4 addresses across four contiguous /24 segments. The current dataset places the casino-domain population as follows:

Sub-range (/24)	Investigated domains	Meaning
185.207.196.0/24	491	Dominant current casino-endpoint segment.

Sub-range (/24)	Investigated domains	Meaning
185.207.197.0/24	2	**Includes SPINSOPOTAMIA.COM at 185.207.197.216.**
185.207.198.0/24	1	Adjacent segment inside the same /22.
185.207.199.0/24	1	Adjacent segment inside the same /22.
Amazon / AS16509	1	genieplay.com only; four other GeniePlay variants remain inside the NALMI /22.

Spinsopotamia.com at 185.207.197.216 therefore occupies the same routed envelope as the wider casino-domain population, even though it does not share the .196/24 host range used by the large majority.

4.4 What the concentration means — and what it does not

A shared /22, ASN and provider create a highly focused infrastructure environment in which a large number of casino-related domains sit behind the same routing and the same provider. That is a material observation: it defines a compact target area for regulators, payment-service providers and infrastructure providers, and it places the Zentoria-facing anchor squarely inside that area.

It does not, however, prove that a single legal entity or customer controls all of these domains. Multiple customers can route inside the same /22; a provider can allocate addresses across many unrelated accounts; and an edge layer such as Cloudflare can sit in front of origins owned by different parties. The infrastructure layer establishes proximity and concentration, not common ownership.

Strongest defensible formulation

Spinsopotamia.com is a Zentoria-facing public anchor whose current endpoint lies inside the same NALMI / AS213846, 185.207.196.0/22 infrastructure envelope as 495 of 496 investigated domains. This is a strong infrastructure bridge. It is not, by itself, proof that Zentoria legally owns all 495 domains.

5. Application Layer: Byte-Identical Asset Clusters

A SHA-256 match means two retained files were byte-for-byte identical at collection time. For generic, provider-managed files this is unremarkable. For application-specific bundles — the JavaScript that builds a casino's own front-end — repeated byte identity across many domains supports a common build artefact, a shared deployment pipeline or a shared platform component. After cleaning, the dataset retained **120 meaningful hash groups**, which form **16 connected technical components** linking **98 domains** across **29 observed brand families**. [PRIMARY]

5.1 Component overview

Every endpoint in every component resolves inside 185.207.196.0/24 and therefore shares the same /22 and provider envelope as the Zentoria-facing 185.207.197.216 endpoint. The byte-identical files add a separate application / deployment correlation layer on top of that shared infrastructure.

Cmp.	Domains	Hash groups	Observed brand families
A	36	49	BoaBoa, Boomerang Casino, BuranCasino, Cadoola, CasinoInfinity, CasinoUnlimited, Castyr, Fezbet, Librabet, Rabona
B	16	13	Casinoly, Joker8, Posido
C	7	4	Casinado, Gozabet
D	4	6	Frumzi
E	4	4	BetRiot
F	4	4	GreatWin
G	4	4	PowerUpCasino
H	3	4	OhMySpins
I	3	1	LuckyElektra
J	3	4	ExciteWin
K	3	4	Playzilla
L	3	4	PolestarCasino
M	2	1	CrazyTower, LolaJack
N	2	11	FunID
O	2	4	LegendPlay
P	2	3	PowBet

5.2 Component A — the largest deployment family

The largest component, Component A, links **36 domains** through **49 separate identical-asset groups**, spanning ten observed brand families: BoaBoa, Boomerang Casino, BuranCasino, Cadoola, CasinoInfinity, CasinoUnlimited, Castyr, Fezbet, Librabet and Rabona. A single shared file (a *dictionary.js* bundle) is byte-identical across all 36 domains; a *vendor.js* bundle is identical across 26. Brand-specific bundles (for example *spaceship_boaboa.js* or *spaceship_cadoola.js*) then cluster sub-groups of domains within the same component. This is the signature of a shared platform emitting near-identical front-end builds across many separately branded skins.

5.3 Other notable components

- **Component B (16 domains, 13 groups):** Casinoly, Joker8 and Posido share a single front-end script across all 16 domains, with brand-specific sub-bundles separating the three families.

- **Component N (2 domains, 11 groups):** the FunID family shows an unusually dense set of shared chunk files and a shared reference to playid.com, suggesting a distinct identity/KYC-style module reused across both domains.
- **Components D–P:** each remaining component binds a single brand family (or a small pair) through its own set of identical runtime, vendor, main and polyfill bundles — the same build emitted across each brand's domain variants.

5.4 The Spinsopotamia limitation

Application-layer boundary for Spinsopotamia.com

Spinsopotamia.com itself contributed **no meaningful shared-asset hash** in the analysed four-VM snapshot, because its public artefact collection was incomplete. The correlation between Spinsopotamia.com and the rest of the network is therefore established primarily through infrastructure data — DNS, prefix and ASN — and not through application-hash matches. Under the no-negative-inference rule, the absent hash is recorded as incomplete collection, not as evidence that Spinsopotamia.com is unrelated to the deployment families. A fresh public asset capture of the domain is a specific recommended follow-up.

The significance of the application layer is therefore twofold. It demonstrates, at PRIMARY weight, that large groups of separately branded casino domains are running byte-identical first-party code — strong evidence of a shared platform or build pipeline. At the same time, it does not by itself link the Zentoria anchor into any specific component, and it does not establish that one legal entity deployed every bundle. Tenant and deployment-account records held by the platform provider would be needed to close that gap.

6. Telemetry Layer: Sentry Replay and Cross-Brand Markers

Fifty-one domains across fourteen observed brand families expose the same public Sentry Replay sampling configuration: ***replaysSessionSampleRate = 0.1*** and ***replaysOnErrorSampleRate = 0.1***. These values are visible in publicly served front-end code and were collected without any interaction with the platforms. **[PRIMARY]**

6.1 Telemetry-marked brand families

Brand family	Domains exposing identical Sentry Replay values
BetRiot	4
Casinado	5
Casinoly	9
ExciteWin	3
Gozabet	2
GreatWin	4
Joker8	5
LegendPlay	2
OhMySpins	3
Playzilla	3
PolestarCasino	3
Posido	2
PowBet	2
PowerUpCasino	4

6.2 Interpretation

Matching sampling values are a configuration-level correlation. They indicate shared or cloned telemetry setups, and they are strongest where they coincide with byte-identical application bundles. In this dataset, all fourteen telemetry-marked families also appear inside the retained asset components — the telemetry layer and the application layer reinforce one another across the same brands.

Identical sampling values do not, however, prove that the same Sentry project, tenant or legal entity controls every listed brand. Two independently operated deployments can share an identical default configuration, particularly if both are built from the same platform template. The telemetry layer therefore corroborates the picture of a common platform without establishing common ownership.

6.3 A separate earlier replay finding

A separate, earlier Betzter-focused analysis recovered a distinct deployment exposing stronger replay settings with global masking controls disabled (*maskAllInputs: false*, *maskAllText: false*, *blockAllMedia: false*). That configuration is recorded as a separate evidence source. It is relevant and important, but it is not automatically projected onto all 496 domains, and it would require project-level confirmation before being generalised. **[SECONDARY]**

6.4 Data-protection relevance

Data-protection relevance

The public Sentry configurations justify provider-side questions about project ownership, authorised users, data retention, cross-brand aggregation and masking policy. Session-replay tooling can capture detailed records of user interaction, and disabled masking controls (where present) raise legitimate questions about whether personal or payment-adjacent data could be recorded. These are questions for the relevant provider and data-protection authority. They do not, on the public evidence alone, establish that any individual user session contained unmasked personal or payment data, nor that any data flow was unlawful.

7. Platform and Service Layer: SPTPub, Analytics, Fraud, Payment and Ancillary Providers

Beyond infrastructure, application code and telemetry, the four-VM corpus records the third-party platform and service components loaded by casino domains. Recurrent use of the same stack across many brands is consistent with a centralised or templated casino-platform environment. Shared third-party services do not prove common ownership, but they identify technical enablers — and potential disclosure targets that may hold decisive tenant and account records.

7.1 Direct platform evidence

Signal	Target	Assessment
trickz.sptpub.com	spinrollz235518.com	Explicit public SPTPub platform-host reference in a saved URLScan result page. One confirmed host in the four-VM packages. **[PRIMARY]**
SPTPub cluster-like strings	16 automatic candidates	Removed as false positives after contextual review; they were Zendesk / Sentry / third-party deployment identifiers.
api.sptpub.com	Hetzner 159.69.41.140/141 (separate earlier report)	Relevant but not newly confirmed by the four-VM packages; cited as a separate artefact. **[SECONDARY]**

7.2 Service footprint across the four-VM corpus

The following services were observed across the corpus. Counts are unique targets on which the service was detected; they indicate breadth of use, not ownership.

Service / layer	Unique targets	Interpretation
Cloudflare	372	Edge, anti-bot, caching and shielding class.
Google Cloud / Storage	300	Content, storage or application-support resources.
AWS / CloudFront	255	Cloud / CDN and campaign / asset delivery.
Google Analytics / Tag Manager	228	Marketing and event instrumentation.
Zendesk / ZD Assets	198	Support, ticketing and customer-retention tooling.
Hotjar	190	Behavioural analytics / session tooling indicator.
SEON	170	Fraud / device-intelligence indicator.
MiFinity	143	Wallet / cashier integration indicator.

Service / layer	Unique targets	Interpretation
Anjouan Gaming components	119	Licensing / seal or compliance-service component class.
Sportradar	59	Sports / data integration indicator.
DeviceInfo	31	Device / profile instrumentation indicator.
SPTPub / Trickz	1	Direct platform-host indicator.
PaymentIQ	1	Direct payment-orchestration indicator.

7.3 The Hetzner boundary

Hetzner (AS24940) appears in 35 saved scan pages across 20 targets and 10 Hetzner IP addresses, but in the parsed URLScan summaries Hetzner was not the main provider for any casino page. Most Hetzner observations relate to consent, advertising or tracking resources. Hetzner is therefore treated as a specific ancillary disclosure target in this corpus, not as the dominant current origin provider.

7.4 Why the service layer matters

The recurrence of the same support tooling (Zendesk), behavioural analytics (Hotjar), fraud-intelligence (SEON), wallet / cashier integration (MiFinity), payment orchestration (PaymentIQ) and a direct platform host (SPTPub) across the population is consistent with a shared operational backend. Each of these providers may hold tenant identifiers, account records and configuration history capable of distinguishing genuinely independent operators from a single centrally managed environment. That is precisely the evidence the public layer cannot supply and that disclosure could.

8. Correlation Matrix: Spinsopotamia / Zentoria vs. the NALMI Casino Network

The following matrix compares, for each evidence layer, the Zentoria-facing anchor against the wider NALMI casino network, and states the remaining gap — the kind of provider-side evidence that would be required to move from technical correlation to legal attribution.

Evidence layer	Zentoria-facing anchor	Wider NALMI network	Remaining gap
Corporate / public facade	Zentoria Limited / Spinsopotamia.com	Prior reporting treats the domain as the key public entry point	Corporate control of the wider 495-domain set not established.
Current DNS / IP	185.207.197.216	Inside the same 185.207.196.0/22 as 495 of 496 domains	Current assignments are snapshots and may change.
ASN / provider	**NALMI / AS213846 envelope**	**Same routing / provider layer for the 495-domain population**	Customer account, billing contact and server allocation undisclosed.
Edge / proxy	Cloudflare in prior header and route evidence	Cloudflare observed on 372 targets	Zone owner, origin shield and WAF rules undisclosed.
Application layer	No retained hash match in current run	120 identical-asset groups connect 98 domains	Fresh public asset capture or provider disclosure required.
Brand / deployment clusters	No direct placement in any of the 16 components	All 16 components reside in 185.207.196.0/24, same /22 as the anchor	Platform / tenant relationship to Spinsopotamia unresolved.
Support / CRM	Prior report records Zendesk, Mailjet, Carmamail indicators	Zendesk assets observed on 198 targets	Account IDs, sender verification and contracting entity undisclosed.
Cashier / payments	Prior report records MiFinity, SwitchPayments, Payabl and xpate context	MiFinity on 143 targets; PaymentIQ on 1 target	MID, gateway, route, acquirer and settlement beneficiary required.

Net assessment

The strongest common point is the infrastructure envelope: prefix, ASN and provider. The strongest wider-network correlation is byte-identical application deployment across 98 domains. The missing decisive bridge is provider-side evidence tying the Zentoria-facing anchor to a specific platform tenant, deployment account, cashier route or contracting entity shared with those asset clusters.

9. Network-Wide Brand and Provider Concentration

The 496 investigated domains collapse into 135 observed domain families under conservative root-name grouping. This is a technical naming inventory, not a legal-entity map: family labels describe naming patterns, not trademark ownership, licensing status or corporate identity. Only two families appear once in the current dataset — DivaSpin and Spinsopotamia — while every other observed label carries two or more domain variants, a pattern consistent with rotating or replacement domains.

9.1 Current origin distribution

As set out in Section 4, 495 of 496 domains resolve inside the NALMI /22, with the single current exception of *genieplay.com* on Amazon / AS16509 — while four other GeniePlay variants remain inside the NALMI /22. The wider use of Google Cloud, AWS / CloudFront and Cloudflare across the corpus reflects ancillary cloud, CDN and edge usage rather than current origin ownership.

9.2 Historical and ancillary provider context

Provider / role	Observed scale	Assessment
Cloudflare / Cloudflare Spectrum	Dominant historical URLScan main-provider and edge presence	Edge, shielding and delivery layer; not current origin ownership by itself. **[BACKGROUND]**
NALMI / AS213846	**495 current domains inside 185.207.196.0/22**	**Primary current infrastructure and disclosure target. [PRIMARY]**
Hetzner / AS24940	35 saved scan pages, 20 targets, 10 IPs; 0 scans where Hetzner was the parsed main provider	Mostly ancillary consent, advertising or tracking infrastructure in this corpus.
Amazon / AS16509	One current apex exception plus widespread third-party AWS / CloudFront resources	Current origin exception for genieplay.com; otherwise ancillary cloud / CDN use.
SPTPub / Trickz	trickz.sptpub.com on spinrollz235518.com	Direct public platform-host reference; one confirmed host in the four-VM packages.

10. Compliance and Regulatory Relevance

10.1 What the findings establish

On the public evidence, this report establishes the following at PRIMARY or SECONDARY weight:

- A highly concentrated casino-domain infrastructure environment under NALMI (AS213846), with 495 of 496 investigated domains inside a single 185.207.196.0/22 prefix.
- A direct infrastructure bridge from the Zentoria-facing Spinsopotamia.com endpoint (185.207.197.216) into that same /22 envelope.
- Sixteen reproducible byte-identical application components connecting 98 domains across 29 observed brand families.
- A cross-brand telemetry marker (identical Sentry Replay sampling) across 51 domains in 14 families, all of which also appear in the asset components.
- A recurring platform and service stack — including an explicit SPTPub platform host and widely repeated analytics, fraud-intelligence, support and payment integrations — consistent with a templated casino-platform environment.

10.2 What the findings do not establish

The report expressly does not establish, and should not be read as establishing, any of the following:

- Common legal ownership of all 496 domains.
- A common ultimate beneficial owner (UBO).
- That Zentoria Limited controls all NALMI customer accounts, or all observed brands.
- That every shared asset or telemetry configuration was deployed or controlled by the same legal entity.
- The identity of the contracting SPTPub, Sentry, Zendesk, Cloudflare, NALMI or payment customer behind any given domain.
- The final merchant, acquirer or settlement beneficiary for any brand.
- Criminal or regulatory liability as a matter of law.

10.3 Implications for stakeholders

Gambling and financial regulators

The concentration defines a compact, testable target area. For a gambling regulator, the question is whether a single licensed perimeter is being used to present many offshore brands to players; for a financial regulator, the question is whether a regulated payment perimeter is being used to route high-risk gambling deposits under benign descriptors. Both questions are answerable from records the named providers hold.

Payment service providers, acquirers and wallet providers

The recurrence of cashier and wallet integrations across the population, together with prior reporting connecting the Spinsopotamia descriptor to a regulated EMI, raises standard merchant-onboarding, gambling-exposure-control, card-scheme-monitoring and transaction-laundering questions. A PSP or acquirer can resolve these against its own MID, gateway, route and settlement records.

Banks and crypto exchanges

Banks and crypto exchanges face the risk of being used as on-ramps or off-ramps for high-risk casino payments presented under clean descriptors. The domain, descriptor and provider indicators in this report can support transaction-screening, descriptor-watchlisting and enhanced due diligence, without any presumption that a given counterparty acted unlawfully.

11. Primary Disclosure Targets and Recommended Follow-Up

The public layer can establish concentration and shared deployment; it cannot establish ownership. The following targets hold the account-level records that would. They are listed by role and by the data types relevant to the technical evidence, without contact details.

Disclosure target	Records required
NALMI Limited / AS213846	Customer(s) controlling 185.207.196.0/22; server allocations; billing and technical contacts; routing agreements; preserved abuse records.
Cloudflare / AS13335	Zone ownership; origin configuration; Ray IDs; DNS history; WAF and abuse records; customer account.
SPTPub / Trickz	Tenant ownership; Brand ID assignment; cluster / start-host assignment; deployment history; authorised users.
Sentry	Project ownership; authorised users; Replay settings; retention and masking configuration.
Zendesk / mail providers	Support tenant; account IDs; sender-domain verification; ticket and campaign routing.
Payment / cashier providers (e.g. MiFinity, PaymentIQ, xpate)	MID; gatewayId; connectorId; routeUuid; acquirer; settlement beneficiary; wallet / cashier tenant.

11.1 Illustrative follow-up questions

The following questions translate the technical evidence into concrete disclosure requests that regulators, PSPs or banks could pose:

- To the infrastructure provider: which customer account(s) control address allocations within 185.207.196.0/22, and do the 491 .196/24 endpoints and the 185.207.197.216 endpoint resolve to the same or to distinct customers?
- To the platform provider: are the domains in Components A–P provisioned under one tenant or several, and does any tenant also account for Spinsopotamia.com?
- To the telemetry provider: do the 51 domains exposing identical Sentry Replay values report into one project / organisation or many, and what masking and retention settings apply?
- To the payment / cashier providers: which MIDs, gateway and route identifiers, acquirers and settlement beneficiaries correspond to the Spinsopotamia descriptor and to the brands in the asset components?
- To the edge provider: what are the origin configurations and zone owners for a representative sample of the casino domains and for Spinsopotamia.com?

11.2 Further OSINT work streams

- A fresh, complete public asset capture of Spinsopotamia.com, to test whether it shares byte-identical bundles with any of the 16 components once collection is complete.
- Passive-DNS and historical-resolution review of the /22 to characterise domain rotation over time.
- Cross-case correlation with other FinTelegram investigations (for example the SPTPub / Betzter platform analysis and prior NovaForge / payment-rail reporting) to test whether the same tenants, descriptors or rails recur.

12. Limitations and Legal Boundary Statement

This report is built on public-source observation and must be read within the limits of that evidence.

- **Snapshot nature.** DNS and IP assignments are time-bound snapshots and may change. URLScan pages can be historical. A third-party hostname appearing in a content-security policy or a saved scan does not prove active use in every user session.
- **Shared infrastructure is not ownership.** A shared provider, ASN, prefix or edge layer does not prove common ownership. A byte-identical first-party bundle is materially stronger evidence of a shared platform or pipeline, but still requires contracting or tenant records for legal attribution.
- **Naming is not identity.** The observed family labels are analyst-normalised from domain names. They describe naming patterns, not trademark ownership, licensing status or corporate identity. Domain variants may be mirrors, replacement domains, country versions or independently configured skins.
- **Incomplete collection for the anchor.** Spinsopotamia.com was incomplete at the application-asset layer in the four-VM run. The anchor relationship therefore relies on current DNS and the separate prior Zentoria evidence set. The report does not invent a shared hash or platform tenant where none was recovered.
- **Separate sources remain separate.** The earlier Betzter replay finding and the api.sptpub.com / Hetzner observation are cited as separate artefacts and are not generalised across the full population without project-level confirmation.
- **Persons named in background.** Any individuals or companies referenced from prior reporting are named without any finding of wrongdoing by this report. They are entitled to the presumption of innocence and to a right of reply.

Publication-grade boundary

This report identifies technical correlations and high-value disclosure targets. All named providers and brands are referred to without any imputation of unlawful conduct. The findings establish a highly concentrated infrastructure environment, a Zentoria-facing infrastructure bridge into that environment, and multiple reproducible deployment correlations. They do not establish common ownership, a common ultimate beneficial owner, a regulatory breach or criminal responsibility. Any such conclusion requires provider-level records and assessment by a competent regulator.

13. Source Bibliography

Technical evidence packages:

- **[01]** Four-VM consolidated public-source evidence package — 496 unique domains; 3,060 manifest-verified files; 838 apex A-record rows; 30,189 CT rows; 959 URLScan references; 1,181 retained public artefacts; 120 meaningful hash groups. Dated 18 June 2026. **[PRIMARY]**
- **[02]** VM1–VM4 final evidence packages — original raw artefacts, worker logs, stage results and SHA-256 manifests. **[PRIMARY]**
- **[03]** Prior Zentoria network-engineer report (Cyprus connection) — identifies Spinsopotamia.com as the Zentoria-facing public anchor; documents 185.207.197.216, the NALMI /22 envelope, active routing, Cloudflare edge indicators and CRM / payment context. Separate source; not generated by the four-VM run. **[SECONDARY]**
- **[04]** SPTPub platform-cluster and Betzter-network technical correlation analysis — design and evidentiary-weight reference; byte-identical assets, telemetry and SPTPub infrastructure. **[SECONDARY]**
- **[05]** Four-VM provider and infrastructure audit — current origin distribution, historical main-provider summaries, ancillary observations, Hetzner scope and service indicators. **[SECONDARY]**
- **[06]** Current DNS and network-distribution tables — Spinsopotamia.com → 185.207.197.216; 495 of 496 domains in 185.207.196.0/22. **[PRIMARY]**

FinTelegram background coverage (narrative framing; allegations and regulator/whistleblower attributions of those sources):

- **[07]** Compliance Report: Zentoria Limited & the NovaForge casino-payment network (Robycasino / Spinsy) — FinTelegram, 19 Feb 2026.
- **[08]** Expanding the Zentoria / NovaForge payment map: Spinsopotamia.com descriptor linked to FCA-regulated EMI xpate — FinTelegram, Mar 2026.
- **[09]** NALMI Ecosphere? Infrastructure signals behind a rotating casino-domain farm — FinTelegram.
- **[10]** Zentoria casino network? Shared rails and Morada Horizon link — FinTelegram, 20 Apr 2026.
- **[11]** Zentoria / NovaForge tag indexes — FinTelegram topic pages.

Final finding

The Zentoria-facing anchor and the wider casino-domain population converge most strongly at the current NALMI /22 infrastructure layer. The wider population is then internally divided into sixteen reproducible application-asset components. The remaining attribution question is which provider, platform, support and payment accounts connect the public Zentoria facade to those deployment components — a question only provider-level records and a competent regulator can answer.

Appendix A — Observed Brand-Family Inventory (selected)

All 496 current domains group into 135 observed families under conservative domain-root normalisation. “NALMI /22” means every listed domain in that family resolves inside 185.207.196.0/22. Families with retained application-hash references are flagged. The full inventory is preserved in the evidence package; a representative selection of the larger and hash-bearing families is reproduced below.

Observed family	Domains	Hash refs	Representative domains
BoaBoa	6	45	boaboa.com; boaboa.biz; boaboa-1993.com; boaboa100-102.com
Boomerang Casino	4	36	boomerang-casino1/8/17/100.com
BuranCasino	6	26	burancasino.com/.biz/.info/.net; burancasino100/855.com
Cadoola	10	72	cadoola2/14/352.com; cad0la-0112–0531.com; 2cadoola.com
CasinoInfinity	4	36	casinoinfinity-0189/1134/1998/4367.com
Casinoly	9	36	casinoly13/14/100/101.com; casin0ly-0100–6330.com
Castyr	2	9	1castyr1.com; 1castyr68.com
ExciteWin	3	12	excitewin.com; excitewin7.com; excitewin-3324.com
Fezbet	5	35	fezbet11.com; fezbet-4549/6212/7138/7147.com
Frumzi	4	23	frumzi8/100.com; 4917-frumzi.com; frumzi756723.com
FunID	2	22	funid-3520.com; funid-6687.com
Gozabet	2	8	gozabet2.com; 6491-gozabet.com
GreatWin	4	16	greatwin1.com; greatwin-0635/5920/5940.com
Joker8	5	25	3/12/14joker8.com; 2755/8395-joker8.com
LegendPlay	2	8	legendplay.com; legendplay1.com
Librabet	4	27	7136-librabet.com; librabet-0123/1817/6728.com
OhMySpins	4	12	0hmyspins-1217/1322/1951/2740.com
Playzilla	3	12	playzilla-0911/1991/8936.com
PolestarCasino	4	12	polestarcasino3/4/5.com; 3862-polestarcasino.com
Posido	5	12	posido270/360/501.com; posido-0638/6539.com
PowBet	2	6	powbet1.com; powbet100.com
PowerUpCasino	4	16	powerupcasino-1131/1201/100/109097.com
Rabona	5	1	rabona101/641.com; 3791-rabona.com; rabona-1826.com
BetRiot	4	16	betriot2/10.com; betriot-1006/1156.com
Casinado	5	20	casinado4/5.com; casinado-4058/6811.com; casinado132456.com
Spinsopotamia	1	—	spinsopotamia.com (anchor; .197/24, no retained hash this run)

Note: a further 100+ families (for example AbuKing, AlfCasino, Cadabrus, Casinia, CrownPlay, MalinaCasino, Neon54, Nomini, Wazamba, YoyoCasino and others) resolve inside the NALMI /22 without retained application-hash references in this run. Their inclusion in the infrastructure population is established by DNS and prefix data; the absence of a retained hash is recorded as incomplete collection, not as disproof.

Appendix B — Retained Hash Inventory Summary

All 120 meaningful cross-domain SHA-256 groups are preserved in the consolidated evidence package, indexed by component. Generic provider-managed files are excluded. The table below summarises the distribution; full SHA-256 values and per-file domain rosters remain in the package.

Component	Domains	Hash groups	Representative shared first-party assets
A	36	49	dictionary.js (36 domains); vendor.js (26); spaceship_{boaboa,cadoola,buran,boomerang}.js
B	16	13	scripts.d661226e….js (16); runtime/main/polyfills (Casinoly 9; Joker8 5; Posido 2)
C	7	4	vendor/runtime/main/polyfills (all 7)
D	4	6	index.runtime.b6c11f21.js + 5 index bundles
E	4	4	polyfills / vendor / runtime / main (BetRiot)
F	4	4	runtime / vendor / main / polyfills (GreatWin)
G	4	4	polyfills / runtime / main / vendor (PowerUpCasino)
H	3	4	polyfills / main / runtime / vendor (OhMySpins)
I	3	1	shared site root (LuckyElektra)
J	3	4	main / runtime / vendor / polyfills (ExciteWin)
K	3	4	main / runtime / vendor / polyfills (Playzilla)
L	3	4	polyfills / vendor / runtime / main (PolestarCasino)
M	2	1	shared site root (CrazyTower / LolaJack)
N	2	11	chunk-*.js ×10 + playid.com reference (FunID)
O	2	4	polyfills / runtime / vendor / main (LegendPlay)
P	2	3	runtime / polyfills / main (PowBet)