Compliance Intelligence Report

SPTPub Platform Cluster and the Betzter Network

A Technical Correlation Analysis

How five outwardly separate online casino brands share byte-identical deployment assets, a common telemetry footprint and direct SPTPub infrastructure links — and what that means for EU regulators, payment providers and data-protection authorities.

Contents

1. Executive Summary

This report documents the results of a passive open-source intelligence (OSINT) correlation scan of seventeen online casino domains. The scan was completed in full — all ten parallel collection workers finished — and produced 711 deduplicated technical markers across 55 hashed public assets, 559 certificate-transparency rows and 133 URLScan references. The analysis isolates two coherent correlation groups.

First, a shared telemetry and deployment stack (Cluster A) links **Betzter** with **Aphrodite, Gambiva, MadCasino and Dracula**. These five domains expose the same FullStory organisation identifier, the same Sentry project, the same InvisibleSport and Pusher hosts, and a byte-identical Livewire application bundle. Four of them additionally share byte-identical Sentry and FullStory bundles.

Second, a set of direct SPTPub integrations (Cluster B) links **BCGame, PlayGlobal, Spartibet and RoxCasino** to a common SPTPub platform identified by the stable cluster marker **c7818b61**. BCGame and PlayGlobal call the same API-K cluster host and share two byte-identical application bundles; Spartibet and RoxCasino call the same API-G cluster and start host while presenting distinct Brand IDs.

The compliance relevance is twofold. The shared telemetry account architecture raises cross-brand player-data aggregation and session-replay questions under the GDPR; the direct SPTPub integrations and distinct Brand IDs are consistent with a shared multi-tenant platform whose tenant, account and settlement records are not publicly visible. The primary disclosure targets are therefore the platform, telemetry, hosting and payment providers that hold the records capable of converting technical correlation into an attributable legal or commercial relationship.

> *This report identifies technical risk indicators, not proven wrongdoing. The findings establish a strong technical relationship between the named domains. They do not establish common legal ownership, a common ultimate beneficial owner, or any regulatory breach or criminal responsibility as a matter of law. All named providers and brands are referred to without any imputation of unlawful conduct, and the presumption of innocence applies throughout.*

2. Methodology and Audit Boundary

The findings were collected through a privacy-safe parallel correlation scan using public sources only. Collection workers queried public DNS, certificate-transparency (CT) logs, URLScan references and public HTTP/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 mechanism was bypassed at any stage.

All ten workers completed successfully. The final evidence package was reconstructed from the completed worker outputs after the original aggregator did not finish its packaging stage; the reconstruction draws only on preserved raw artefacts and does not introduce any new collection. Collection produced 711 deduplicated marker rows, 55 hashed public assets, 559 CT rows, 253 DNS rows and 133 URLScan references across 17 target domains.

2.1 Worker completion

Stage	Requests	Successful	Failed
crt.sh (certificate transparency)	17	3	14
public-html	17	9	8
public-js	46	46	0
urlscan-detail	133	0	133
urlscan-result-page	133	59	74
urlscan-search	17	17	0

2.2 Evidence integrity controls

- Every collected file was hashed with SHA-256 at collection time.
- The shareable package contains a SHA-256 manifest and excludes the local run-state file that contained a workstation path, so no source-identifying environment data is published.
- Raw public artefacts, worker logs, stage results and the reconstructed aggregate CSV files are preserved together.
- The final package hash can be independently verified before transfer. Evidence package SHA-256: **D1318E7A…2FCDBBF**; run ID: **Run20260615140057**.

2.3 Source failures and the no-negative-inference rule

Several public sources were rate-limited or unavailable during the run. URLScan detail retrieval was affected by HTTP 429 rate limits and HTTP 403 responses; certificate-transparency collection returned HTTP 502 errors and timeouts for several domains; and some direct public fetches were blocked with HTTP 403, reducing JavaScript and HTML coverage. A failed CT call does not mean that no certificates exist, and a blocked fetch does not mean that a marker is absent.

> **No negative inference from missing data**

A source failure or a missing marker is recorded as unavailable or incomplete. It is never treated as proof that a relationship does not exist. Every interpretation in this report carries the limitations of the run with it.

3. Evidentiary Weight System

Every evidentiary claim in this report is graded with one of four tiers. The tier reflects how the underlying observation was established, not the seriousness of any inference drawn from it.

Tier	Definition
PRIMARY	Verified via forensic network evidence — byte-identical SHA-256 hashes, direct API hostnames, or stable cluster markers recovered from public artefacts.
SECONDARY	Corroborated by two or more independent non-primary sources.
LEAD	A single-source OSINT indicator that has not yet been independently verified.
BACKGROUND	Publicly available contextual information.

Tags appear in brackets after each finding, for example. Cloudflare edge addresses, generic CDN scripts, provider-managed anti-bot files and wildcard DNS are treated as low-weight or excluded entirely from ownership conclusions.

4. Finding A — Shared Telemetry and Deployment Stack (Cluster A)

Aphrodite, Gambiva, MadCasino and Dracula expose the same principal telemetry and deployment artefacts. Betzter joins this group through a byte-identical Livewire application bundle and the same core telemetry identifiers.

4.1 The five-domain technical fingerprint

The following markers were recovered across betzter.com, aphrodite.casino, gambiva.com, madcasino.io and dracula.casino.

Marker	Value	Weight
FullStory Org ID	o-23D3EG-na1	**PRIMARY**
Sentry project ID	4504971543642112	**PRIMARY**
Sentry public key	7363894271784a978de7f4e11b0640bd	**PRIMARY**
InvisibleSport host	ui.invisiblesport.com	**PRIMARY**
Pusher host	ws-eu.pusher.com	**PRIMARY**
Shared Livewire asset SHA-256	301E73159E53ADAB3A713C8DD4DAA43EA2C2E15164E5B757774BE2E38ED52DA2	**PRIMARY** — byte identity across 5 domains

Aphrodite, Gambiva, MadCasino and Dracula additionally share four byte-identical Sentry and FullStory bundles that were not observed on Betzter in this run. This is consistent with a slightly different deployment state for Betzter while the core telemetry identifiers — the FullStory organisation, the Sentry project and the InvisibleSport host — remain common to all five.

4.2 Betzter's additional player-event markers

Betzter contains the most complete combination of player-event, telemetry and third-party identifiers within Cluster A. The following markers were recovered from its public application JavaScript.

Marker	Value	Weight
Pusher key	057098928717a40e62b9	**PRIMARY**
Private channel patterns	playerAccount.{uuid}; playerAccount.{uuid}.sessions	**PRIMARY**
Player-linked fields	Player.uuid; Player.email	**PRIMARY**
Event marker	PlayerAccountUpdatedBalance	**PRIMARY**

Marker	Value	Weight
Sentry Replay config	maskAllInputs: false; maskAllText: false; blockAllMedia: false; replaysSessionSampleRate: 0.05; replaysOnErrorSampleRate: 1	**PRIMARY**

The compliance significance is that player-identity fields are linked to session telemetry, and that telemetry is aggregated under a single FullStory organisation account observed across five brands. The markers demonstrate the capability to associate session and application telemetry with player-account identifiers. They do not, on their own, establish how every session was actually processed.

4.3 KingdomCasino Austria (kingdomcasino4.io)

The FullStory Org ID **o-23D3EG-na1** was observed on kingdomcasino4.io (the Austrian KingdomCasino domain). This is recorded as a single-marker indicator.

The related domains kingdomcasino.io (main), kingdomcasino6.io (NL) and kingdomcasino16.io (IT) returned INCOMPLETE in this run because their public sources were unavailable. Consistent with the no-negative-inference rule, this is not evidence that those domains lack the marker.

4.4 Assessment and interpretive boundary

Assessment — MEDIUM to MEDIUM-HIGH technical correlation

Repeated telemetry identifiers and byte-identical application bundles are materially stronger evidence than visual similarity or shared CDN hosting. They point to a shared deployment pipeline, a shared telemetry account, or both. Ownership of the telemetry accounts, the deployment pipeline and the underlying platform relationship remains unresolved pending provider disclosure.

5. Finding B — Direct SPTPub c7818b61 Cluster Integrations

Four reference domains expose direct SPTPub API or start-host integrations that contain the stable cluster marker c7818b61. Direct API hostnames and distinct Brand IDs are among the strongest reproducible indicators in the dataset.

5.1 Four reference domains

Brand (reference)	Domain	Direct SPTPub hosts	Brand ID
BCGame	bcgame51.com	api-k-c7818b61-623; start9	2103509236163162112
PlayGlobal	playglobal7.com	api-k-c7818b61-623; start9	—
Spartibet	spartibet.com	api-g-c7818b61-607; start5	26199778140987146311
RoxCasino	roxcasino5008.com	api-g-c7818b61-607; start5	1893391418244866048

BCGame and PlayGlobal share two byte-identical application bundles — **Enter-Bt9QyBH_.js** (F55CEB0E…) and **index-D1WAJYnV.js** (5A5D3903…) — alongside the same direct SPTPub API-K host and start9 host.

5.2 Multi-tenant inference

Spartibet and RoxCasino call the same API-G cluster and the same start5 host but expose different Brand IDs. This is consistent with separate tenant or brand configurations operating on a shared platform. The inference is structural and must be confirmed against internal platform records.

5.3 Relationship to Cluster A

> The Cluster B reference domains are not currently attributed to Softon Ltd or to any identified Softon-associated entity. They are documented here because they share the SPTPub platform infrastructure that is referenced in Betzter's public application layer (the sptpub.com marker observed in Betzter's Sentry configuration). They are relevant as platform-ecosystem context and as anchors for provider disclosure, not as evidence of common ownership with Cluster A.

[1]Brand ID variance noted in source: the Finding B table (p.7 of the source) and the analyst brief record 2619977814098714631; the Domain Assessment Matrix (p.10) records 2619977814098714624. The …631 value is used here pending reconciliation against SPTPub tenant records.

6. Byte-Identical Asset Evidence

The retained hashes below support correlation of application-specific bundles. Generic Cloudflare challenge JavaScript and provider-managed assets are excluded from the primary attribution analysis, because such files can appear across entirely unrelated websites.

Asset / bundle	Domains observed across	SHA-256 prefix	Classification
livewire.min.js	aphrodite.casino; betzter.com; dracula.casino; gambiva.com; madcasino.io	301E73159E53ADAB3A…	**Retained**
sentry-release-injection-file	aphrodite.casino; dracula.casino; gambiva.com; madcasino.io	4EF3F856A70EEF5E78…	**Retained**
index-D1WAJYnV.js	bcgame51.com; playglobal7.com	5A5D390309393C5442…	**Retained**
fullstory-187b7e91.js	aphrodite.casino; dracula.casino; gambiva.com; madcasino.io	73816A7D7EDE501F67…	**Retained**
main.js	aphrodite.casino; bcgame51.com	B6BBC4AF2D7BBECE3A…	Excluded — generic provider asset
sentry-0068992d.js	aphrodite.casino; dracula.casino; gambiva.com; madcasino.io	CAA7B80215BC153610…	**Retained**
Enter-Bt9QyBH_.js	bcgame51.com; playglobal7.com	F55CEB0E8F30AE2218…	**Retained**

Why byte identity matters

- A SHA-256 match means the collected files were byte-for-byte identical at collection time.
- For application-specific bundles, repeated byte identity is strong evidence of a shared build artefact, a shared deployment pipeline or a common platform component.
- Attribution weight depends on the asset type. Provider-managed CDN and anti-bot files carry low value; application bundles and project-specific telemetry files carry higher value. The main.js match above is therefore excluded, while the Livewire and SPTPub bundles are retained.

7. Data Protection and Consumer Risk Assessment

7.1 Cross-brand player-data aggregation risk

The shared FullStory Org ID **o-23D3EG-na1** means that if five casino brands feed into the same FullStory organisation account, player behavioural data — potentially including **Player.uuid** and **Player.email** — is aggregated under a single account across multiple casino brands without, on the publicly available evidence, any disclosed consent basis for cross-brand data sharing.

This pattern raises questions under the GDPR: Article 5 (purpose limitation, where data collected for one brand may be processed in a wider cross-brand context), Article 13 (transparency toward the data subject about who controls the data and for what purpose), and Article 25 (data protection by design and by default). The assessment reflects the configuration observed in public artefacts; it does not establish how the FullStory organisation is contractually structured.

> **Risk rating — HIGH**
> Cross-brand aggregation of identity-linked behavioural data under a single telemetry account, with no publicly disclosed consent basis for the sharing.

7.2 Session replay with masking controls disabled

Betzter's Sentry Replay configuration was recovered with **maskAllInputs: false**, **maskAllText: false** and **blockAllMedia: false**, with session-replay sampling configured (replaysSessionSampleRate 0.05; replaysOnErrorSampleRate 1). Text fields and inputs — which on a gambling platform may include personal data, financial amounts and login credentials — are therefore not globally masked in session recordings under the recovered configuration.

> **Risk rating — HIGH (Betzter deployment)**
> This is a configuration-level finding. It indicates that masking controls were not globally enforced in the recovered replay configuration; it is not proof that every session actually captured unmasked personal data.

7.3 AML and profiling risk

The mapping of **Player.uuid** and **Player.email** to balance-update events (**PlayerAccountUpdatedBalance**) enables granular, player-level behavioural profiling. In the context of an offshore-licensed operator with opaque beneficial ownership, this data architecture raises questions about who has access to the aggregated player intelligence and for what purpose.

> **Risk rating — MEDIUM-HIGH**
> Identity-linked balance-event telemetry supports detailed player profiling; the controller of the aggregated data and the access controls around it are not visible on public evidence.

8. Compliance and Regulatory Relevance

8.1 What the findings establish

The findings establish a strong technical relationship between the named casino domains: shared telemetry identifiers and byte-identical application bundles within Cluster A, and direct SPTPub platform integrations with distinct Brand IDs within Cluster B. They do not establish common legal ownership, a common ultimate beneficial owner, or any specific regulatory breach as a matter of law.

8.2 What the findings do not establish

- Common legal ownership of any of the named brands.
- The identity of the contracting SPTPub, FullStory, Sentry or Pusher customer.
- Whether every user session contained unmasked personal data.
- The final payment processor, merchant account, acquirer or settlement beneficiary for any brand.

8.3 Primary disclosure targets

The next decisive evidence is held by the platform, telemetry, hosting and payment providers. The records most likely to convert technical correlation into an attributable relationship are set out below.

Disclosure target	Records required
SPTPub	Tenant configuration, Brand ID assignment, API cluster assignment, deployment history and account ownership.
FullStory	Organisation o-23D3EG-na1 — ownership, contracting entity, authorised users and any data-sharing arrangements across brands.
Sentry	Project 4504971543642112 — ownership, contracting entity and authorised users.
Pusher	Application 057098928717a40e62b9 — account owner and contracting entity.
Hosting provider (Hetzner AS24940; 159.69.41.140/141)	Customer account, billing contact, routing metadata and preserved abuse-channel / access logs.
Payment and cashier providers	No MID, gatewayId, connectorId, routeUuid or acquirer was identified across 1,020 public path checks. The cashier route is a documented gap and a primary disclosure target.

9. Investigative Next Steps

- Repeat the blocked CT, URLScan and direct-fetch stages for the incomplete domains — kingdomcasino.io, kingdomcasino6.io, kingdomcasino16.io, wildzy.io, wino.casino, tucancasino.com and smash.casino — under ordinary rate limits, preserving each run separately.
- Verify FullStory Org ID reuse across any further casino domains beyond those captured in this run.
- Correlate the SPTPub Brand IDs with cashier / PSP routes and settlement beneficiaries.
- Request provider confirmation of the FullStory organisation, the Sentry project, the Pusher application and the SPTPub tenant ownership.
- Capture SSL/TLS certificate SANs and CT history for api.sptpub.com and associated hostnames.
- Reconcile the HTTP 403/404 discrepancy on 159.69.41.140 with a fresh, timestamped capture.

Primary disclosure logic

Another broad scan is less valuable than controlled disclosure of tenant, account and payment-routing records. The decisive next step is provider-side confirmation, not further passive collection.

10. Source Protection and Methodology Statement

The technical findings in this report were collected through passive OSINT methods. No account was created, no login was performed, no payment flow was initiated, no authentication endpoint was tested, and no non-public system was accessed.

All collected files were hashed with SHA-256. The evidence package (**Run20260615140057**, SHA-256: **D1318E7A…2FCDBBF**) is preserved with full integrity controls and can be independently verified before transfer.

Source-protection provisions apply, and no information capable of identifying a technical source is published. This report is classified CONFIDENTIAL — JOURNALISTIC PRIVILEGE and is prepared in furtherance of public-interest compliance reporting under applicable journalistic source-protection provisions, including the protections recognised in Article 10 ECHR jurisprudence.

11. Source Bibliography

01 — Passive OSINT evidence package Run20260615140057. 17 target domains, 10/10 workers completed, 711 deduplicated markers, 55 hashed public assets, 559 CT rows, 133 URLScan references. SHA-256 evidence package: D1318E7A…2FCDBBF. Date: 15 June 2026. PRIMARY — forensic network evidence. On file with FinTelegram.

02 — Public JavaScript assets, betzter.com — FullStory Org ID o-23D3EG-na1, Sentry project 4504971543642112, Pusher key 057098928717a40e62b9, player-event and channel markers. Captured passively June 2026. PRIMARY — public application layer.

03 — Public JavaScript and HTML assets, aphrodite.casino, gambiva.com, madcasino.io, dracula.casino — shared FullStory, Sentry, Livewire, InvisibleSport and Pusher markers; byte-identical application bundles. Captured passively June 2026. PRIMARY — public application layer.

04 — Public application layer, bcgame51.com — direct SPTPub API host api-k-c7818b61-623.sptpub.com, Brand ID 2103509236163162112, byte-identical bundles with playglobal7.com. PRIMARY — direct API hostname.

05 — Public application layer, playglobal7.com — api-k-c7818b61-623.sptpub.com, byte-identical bundles with bcgame51.com. PRIMARY — direct API hostname.

06 — Public application layer, spartibet.com — api-g-c7818b61-607.sptpub.com, start5, Brand ID 2619977814098714631. PRIMARY — direct API hostname.

07 — Public application layer, roxcasino5008.com — api-g-c7818b61-607.sptpub.com, start5, Brand ID 1893391418244866048. PRIMARY — direct API hostname.

08 — Public application layer, kingdomcasino4.io — FullStory Org ID o-23D3EG-na1 observed. LEAD — single marker, run incomplete for other KingdomCasino domains.

09 — Certificate Transparency data, URLScan references and DNS records for 17 target domains. Captured June 2026 via crt.sh, URLScan and public DNS resolvers. PRIMARY for DNS; SECONDARY for CT/URLScan (partial — rate-limited).

12. SEO Metadata Block

For the web-publication build. This block is separate from the main report text and is not for the internal review build.

Field	Value
SEO Title	SPTPub Platform Cluster and the Betzter Casino Network — Technical Correlation Analysis
Meta Description	FinTelegram forensic analysis reveals byte-identical application assets, shared FullStory and Sentry telemetry, and direct SPTPub infrastructure links connecting Betzter with Aphrodite, Gambiva, MadCasino and Dracula casinos.
URL Slug	sptpub-betzter-casino-network-technical-correlation-analysis
Primary Keywords	SPTPub, Betzter, FullStory casino telemetry, Sentry casino, shared casino platform, iGaming OSINT
Secondary Keywords	Softon Ltd, passive OSINT compliance, casino brand correlation, EU iGaming AML, FinTelegram
Category	Compliance / iGaming / Network Forensics
Tags	SPTPub, Betzter, Aphrodite casino, Dracula casino, MadCasino, Gambiva, FullStory iGaming, passive OSINT, EU compliance

Editorial standard

This report does not assert that any named person or entity has committed a criminal offence. It does not state that SPTPub, InvisibleSport, NovaFlick, FullStory, Sentry or Pusher own or operate any casino brand. It does not assert common legal ownership from technical markers alone. All assessments describe the strength of technical correlation within the collected public artefacts; they are not legal findings, licensing determinations or statements of criminal responsibility.