

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

vainabet.io

Objeto investigado	vainabet.io - cassino e apostas “VAINABET”
Natureza	Verificação do regime de operação no Brasil e de vínculos com outros domínios
Data da coleta	28/11/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bases públicas, análise do código da página)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do HTML e dos scripts
Achado central	Cassino em português com depósito por Pix, operado por empresa declarada na Costa Rica com licença de Anjouan, que compartilha o mesmo código com **outros quatro cassinos**
Classificação	**RISCO ALTO**
Emissão do laudo	28/11/2026 as 01:06

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **vainabet.io**, realizada em **28/11/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem cadastro, sem compra e sem envio de dados pessoais. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O `vainabet.io` foi registrado em 20/05/2026 (Immaterialism Limited (IANA 802672)), está atrás da Cloudflare e publica um cassino com apostas esportivas em português (`lang="pt-BR"`). O código da página trata depósito e saque por **Pix**, pede CPF e exige que a chave Pix esteja no nome do apostador.

O rodapé atribui a operação à “Enigma Digital Solutions Limitada”, em San José (Costa Rica), “licenciada” pelo governo da ilha de Anjouan (Comores). Licença estrangeira não autoriza a oferta de apostas no Brasil, que exige autorização da SPA/MF e domínio .bet.br; `vainabet.bet.br` não existe.

A página é a mesma aplicação Next.js de `zezao.net`, `metaigaming.io`, `v10.bet`, `brotabet.co`: 28 dos 29 arquivos de script são idênticos, as imagens vêm do mesmo servidor (`cdn.meta-img.xyz`) e o rodapé é o mesmo. O RDAP do registro `.io` informa o titular com endereço no **Brasil (RJ)**, apesar do operador declarado na Costa Rica.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: são várias marcas sobre uma única plataforma, o que permite trocar de nome quando um domínio é bloqueado; nenhuma tem autorização brasileira.

2. Metodologia e Cadeia de Custódia

Empregaram-se exclusivamente **técnicas passivas**. As respostas de rede e de bases públicas foram salvas no momento da coleta e tiveram hash SHA-256 calculado. O DNS foi consultado via resolvedor público 1.1.1.1; o conteúdo, os cabeçalhos e o bundle JavaScript foram obtidos por requisição HTTPS de visitante comum. Nenhum formulário foi preenchido e nenhum dado pessoal foi enviado. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (rdap.org / registro do gTLD / Registro.br)	`rdap_raw.json · rdap_*.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante comum) e navegador headless; home, páginas legais e scripts	`corpo_*.html · headers_home.txt · bundle*.txt`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`geoip.json`
CNPJ declarado	Validação por módulo 11 · base pública BrasilAPI/Receita	`cnpj_publico_*.json`
Consolidação	Extração de fatos e hashes SHA-256	`hash_manifest.txt`

3. Identificação Técnica (Domínio, DNS, Hospedagem e TLS)

Domínio	vainabet.io
Registro	20/05/2026 · expira 20/05/2028 · **192 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)

Registrador	Immaterialism Limited (IANA 802672) ·
Servidores de nome	jake.ns.cloudflare.com · ophelia.ns.cloudflare.com
DNS - A	104.21.50.33 · 172.67.199.245 · sem MX
Hospedagem	AS13335 Cloudflare, Inc. · San Francisco/US · cabeçalho `server: cloudflare`
Certificado TLS	Google Trust Services (WE1) · emitido em 01/11/2026 · válido até 30/01/2027
Rodapé	“Meta é operado pela Enigma Digital Solutions Limitada… San Jose, Costa Rica. Licenciado… pelo Governo da Ilha Autônoma de Anjouan”
Código compartilhado	28 de 29 arquivos Next.js idênticos aos de `zezao.net`, `metaigaming.io`, `v10.bet`, `brotabet.co`
Domínio .bet.br	`vainabet.bet.br` — NXDOMAIN

Leitura: domínio de 192 dias com titular oculto, atrás da Cloudflare.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Aplicação Next.js com rastreamento de campanhas (Utmify, Facebook Pixel, Google Tag Manager) e chat de atendimento (Digisac, Intercom, LiveChat).

Aspecto	Constatação
Pagamento	Depósito e saque por Pix, com CPF
Operador declarado	Enigma Digital Solutions Limitada (Costa Rica)
Licença declarada	Anjouan (Comores), sem número verificável na página
Marcas irmãs	`zezao.net`, `metaigaming.io`, `v10.bet`, `brotabet.co`

Leitura: o apostador deposita por Pix em operador estrangeiro sem autorização no Brasil, sem a proteção da regulamentação nacional.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Cassino em português com depósito por Pix ao público brasileiro fora de domínio .bet.br	`corpo_home_resolve.html`	ALTA
2	Mesmo código (28 de 29 arquivos) de outros quatro cassinos com outros nomes	`rede_comparacao.txt`	ALTA
3	Operador declarado no exterior com licença de Anjouan, sem autorização brasileira	`corpo_home_resolve.html`	MEDIA
4	Domínio com titular oculto, 192 dias antes da coleta	`rdap_raw.json`	BAIXA

Síntese: 4 indicadores, 2 de severidade alta.

6. Conclusão Técnica e Recomendações

O vainabet.io oferece cassino e apostas com depósito por Pix ao público brasileiro, fora do regime autorizado pela SPA/MF, como uma de pelo menos cinco marcas sobre a mesma plataforma. Classificação técnica: **RISCO ALTO**.

Recomendações ao consumidor / solicitante

- No Brasil, só operam legalmente as casas de apostas autorizadas pelo Ministério da Fazenda, sob domínio `.bet.br`; consulte a lista oficial da SPA/MF antes de depositar.
- Não instale aplicativos (APK) baixados fora das lojas oficiais nem informe CPF e dados bancários a operadores sem identificação verificável.
- Em disputa com operador fora do regime autorizado, o apostador não conta com a proteção da regulamentação brasileira para reaver saldo ou saques.

Recomendações de mitigação / denúncia

- Reportar o endereço ao Google Safe Browsing e ao canal de abuso do registrador (-).
- Comunicar à Secretaria de Prêmios e Apostas (SPA/MF) e à Anatel a oferta de apostas ao público brasileiro fora do regime autorizado.
- Vítimas que pagaram via Pix: acionar o banco imediatamente pedindo o MED (Mecanismo Especial de Devolução), registrar boletim de ocorrência e reclamação em consumidor.gov.br / Procon, anexando este laudo.

Ressalva: este laudo expressa **juízo técnico de risco** com base em evidências públicas coletadas passivamente em 28/11/2026; não é decisão judicial e não imputa crime a nenhuma pessoa física ou jurídica. Registradores, provedores de hospedagem/CDN,

plataformas de loja e intermediários de pagamento são citados apenas como fatos técnicos, sem imputação de conduta. O titular do site pode usar estes achados para corrigir as inconsistências apontadas. Os fatos podem mudar após a coleta.

Anexo A - Manifesto de Integridade (SHA-256)

Hashes SHA-256 das evidências preservadas no momento da coleta (cadeia de custódia).

Arquivo	SHA-256
bet_br_check.txt (214 bytes)	92cc5f40a4c9da542759dd56e9b3eef3f83c8c132463c448705a4018605abc81
bundle_js.txt (398017 bytes)	bb1e0ee328e0537400e4b29826bcab977170133ef6bdb993310531b6356adf97
corpo_home.html (47011 bytes)	e4ddfb5d5624a004c06ce40700b3734daf3f4a13d20b95de9e2e2249f91fb5df
corpo_home_resolve.html (47011 bytes)	e4ddfb5d5624a004c06ce40700b3734daf3f4a13d20b95de9e2e2249f91fb5df
dns_records.txt (359 bytes)	d91b91d7ae5d0ce73bd4698d9cacde3dc20425224a125285bb58143ee0fdf5f1
geoip.json (287 bytes)	2b96a44f5368660e56862b9ba814ec6d002f31f53b60592acc38294c8f7a5322
headers_home.txt (1063 bytes)	3d56a6fc7ea077414764194f6e21eb67c60d0252c4e423819f74ac3144b1a549
headers_home_resolve.txt (1029 bytes)	88a8bd1a4e2ddfc38bd1e58cdd92807e117c499f416e9c3bfbd6238d0e19cda8
rdap_raw.json (9037 bytes)	315935b8dbe4f12579c1e40c38a7b5053e70ba9572518f910076d9c94eacd8f7
rede_comparacao.txt (502 bytes)	f29ddd33909aaaf311676813d61f939a9033b4ed96358b83780cf17bd2b78e58
resolvedores.txt (221 bytes)	b188b93e74dbe476e55faa2ccc3b5b5e3d61a6f692134eac94bc6357aca3834d
tls_cert.txt (300 bytes)	97a5fbed865eea0c4e1a59841cd1f5242334ea177ca3de9a877419bdd0d03826

- Fim do relatório -