RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

betouganhou.com

Objeto investigado	betouganhou.com — casa de apostas esportivas e cassino ao vivo (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor + análise do PIX de checkout
Data da coleta	06/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, app e código PIX)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do app · decodificação BR Code (EMV)
Achado central	Apostas/cassino SEM operador identificado e SEM autorização; PIX recebido por terceiro ("KOKISCOMPRA") que NÃO corresponde à marca
Classificação	**RISCO ALTO**
Emissão do laudo	06/07/2026 às 13:43

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **betouganhou.com**, realizada em **06/07/2026** por técnicas de OSINT e análise passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem interação intrusiva. Além da análise do site, decodificou-se o **código PIX "copia e cola"** da tela de pagamento fornecida pelo solicitante. Toda evidência foi preservada em arquivo com hash SHA-256 (cadeia de custódia).

O domínio **está no ar** e entrega uma **casa de apostas esportivas e cassino ao vivo** em português (título: "Betou, Ganhou! – Apostas Esportivas e Cassino ao Vivo"), construída como aplicação de página única (**SPA React/Vite**) servida pela **Vercel**, com back-end em **Supabase** (`leoroqxlqhyaayfzhdex.supabase.co`) e funções de **depósito/saque via PIX**. O rodapé traz apenas "© 2026 Betou, Ganhou!", **sem CNPJ, razão social ou endereço**, e não há canal de contato corporativo identificável.

A tela de pagamento aponta para um **PIX dinâmico** intermediado pelo gateway `qrcode.a55scd.com.br`, cujo domínio pertence à **SELECT CREDIT SCMEPP LTDA** (CNPJ 45.756.448/0001-78, ligada à processadora **Pagsmile**) — uma instituição de pagamento regular. Ponto crítico: o **nome do recebedor no código PIX é "KOKISCOMPRA"** (São Paulo), um terceiro que **não corresponde à marca anunciada** "Betou, Ganhou!". Ou seja, o dinheiro do apostador é coletado, via um gateway legítimo, em nome de **uma empresa diferente e opaca** — padrão comum de sites de aposta irregulares que roteiam PIX por sub-lojistas genéricos.

Juridicamente relevante: no Brasil, apostas de quota fixa e cassino online dependem de **autorização federal** do Ministério da Fazenda (SPA/SIGAP, Lei 14.790/2023), e as casas autorizadas operam sob o domínio padronizado **.bet.br**. Este site usa **.com** genérico, foi **registrado há ~11 dias** (25/06/2026), tem **titular oculto** e **nenhum indício de autorização** — perfil compatível com **operação irregular/não autorizada**, categoria sujeita a bloqueio pelas autoridades brasileiras.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: uma casa de apostas que recebe dinheiro (PIX) e dados de usuários **sem identificar quem a opera nem comprovar autorização**, e cujo **recebedor do PIX é um terceiro sem relação aparente com a marca**, oferece **risco elevado** — ausência de responsável localizável e de garantia de pagamento de prêmios/saques. Recomenda-se **não cadastrar, não depositar e não fornecer dados** (Seções 6 e 7).

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 registro dos domínios foi consultado por **RDAP** (Verisign para o .com; Registro.br para o .com.br do gateway); o DNS por `dig`; o conteúdo e os cabeçalhos por requisições HTTPS de navegador; o certificado por `openssl s_client`; a geolocalização por ipinfo.io e ip-api.com; e o **código PIX** por decodificação do padrão EMV/BR Code (TLV), com verificação do CRC16. Não houve cadastro, depósito nem login. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Verisign / .com — registrador Dynadot)	`rdap_main.json`
DNS	dig (A, NS, MX)	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (site e assets)	`corpo.html · headers.txt`
Aplicação (front-end)	Download dos bundles JS/CSS (Vite)	`mainapp.js · assets/*.js`
Certificado TLS	openssl s_client / x509	`ssl_cert.txt`

Geolocalização do IP	ipinfo.io · ip-api.com	`ipinfo.json · ipapi.json`
Gateway de pagamento	RDAP + DNS (a55scd.com.br / qrcode.a55scd.com.br)	`rdap_gw.json · dns_gw.txt`
Código PIX (checkout)	Decodificação EMV/BR Code (TLV) + CRC16	`pix_decode.txt · pix/ (print)`

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

Domínio	betouganhou.com (gTLD .com — Verisign)
Registro	**25/06/2026** · expira 25/06/2027 · última alteração 26/06/2026
Idade na coleta	**~11 dias** — domínio muito recente
Titular	**Oculto** (privacidade de registro; RDAP expõe só o registrador)
Registrador	Dynadot Inc
Status	clientTransferProhibited
Servidores de nome	ns1 / ns2.vercel-dns.com (DNS gerenciado pela Vercel)
DNS — A	64.29.17.65 · 216.198.79.1 (Vercel/AWS, anycast) · sem MX
Hospedagem	AS16509 Amazon (AWS) sob a plataforma **Vercel, Inc.** · Server: Vercel
Back-end de aplicação	Supabase — `leoroqxlqhyaayfzhdex.supabase.co` (funções de depósito/PIX)
Geolocalização do IP	Anycast Vercel (não revela a localização do operador real)
Certificado TLS	CN=*.betouganhou.com (wildcard) · emissor Let's Encrypt YR1 (DV) · válido 25/06/2026–23/09/2026

Leitura técnica. Registro **de apenas ~11 dias**, validade de 1 ano e titular oculto compõem um perfil de **baixa rastreabilidade do responsável**. A hospedagem na **Vercel** (serverless sobre AWS) e o back-end **Supabase** são infraestrutura legítima e de uso comum — não constituem, por si, indício de fraude, mas o modelo **anycast/serverless não revela a localização de quem opera**. O certificado **wildcard DV gratuito** comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. Não se imputa conduta ao registrador (Dynadot), à Vercel, à Amazon (AWS) nem à Supabase, meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site entrega uma **casa de apostas esportivas e cassino ao vivo** em português (SPA React/Vite), com depósito, saque, bônus e áreas de apostas/cassino. O back-end é **Supabase**, e o fluxo financeiro usa **depósito via PIX** através de funções de borda (Edge Functions). O único e-mail técnico não corporativo e a ausência de CNPJ/endereço indicam **operador não identificado**. Há textos genéricos de "18+" e "Jogo Responsável", mas nenhuma identidade de empresa ou selo de autorização.

4.1. Decodificação do código PIX (checkout)

O código "copia e cola" da tela de pagamento foi decodificado pelo padrão **EMV/BR Code (TLV)**; o **CRC16 confere** (56F7), confirmando a integridade do payload:

GUI / arranjo	br.gov.bcb.pix (PIX)
Tipo	PIX **dinâmico** (Point of Initiation 12) — payload por URL
Gateway (URL payload)	`qrcode.a55scd.com.br/v1/cc904fac-…-1266d983ce75`
Nome do recebedor (campo 59)	KOKISCOMPRA — **não** corresponde à marca "Betou, Ganhou!"
Cidade (campo 60)	SAOPAULO
MCC (campo 52)	0000 (categoria não especificada)
Moeda / País	986 (BRL) / BR
CRC16 (campo 63)	56F7 — **válido** (íntegro)

O domínio do gateway `a55scd.com.br` está registrado (Registro.br) em nome da **SELECT CREDIT SCMEPP LTDA** — CNPJ **45.756.448/0001-78**, contato técnico ligado à processadora **Pagsmile** (`@pagsmile.com`); `qrcode.a55scd.com.br` resolve em AWS São Paulo. Trata-se de **instituição de pagamento regular**: a ela não se imputa conduta. O sinal de alerta está na **divergência entre o recebedor ("KOKISCOMPRA") e a marca anunciada** — o valor pago para "apostar no Betou, Ganhou!" é, na prática, coletado por um **terceiro opaco** por trás do intermediário.

Aspecto	Constatação
Tipo de serviço	Apostas esportivas + cassino ao vivo ("Betou, Ganhou!")
Tecnologia	SPA React/Vite na Vercel · back-end Supabase (Edge Functions de depósito/PIX)
Meio de pagamento	Depósito via PIX (dinâmico) intermediado por qrcode.a55scd.com.br
Intermediário (gateway)	SELECT CREDIT SCMEPP LTDA / Pagsmile (CNPJ 45.756.448/0001-78) — instituição regular
Recebedor do PIX	**"KOKISCOMPRA"** — terceiro que NÃO corresponde ao estabelecimento anunciado
Dados coletados	Cadastro/login e carteira via Supabase (dados de conta, e-mail; dados de saque no fluxo autenticado)
Identificação do operador	**Ausente** — rodapé só "© 2026 Betou, Ganhou!"; sem CNPJ, razão social ou endereço
Autorização / licença	**Ausente** — sem selo SPA/SIGAP; domínio .com, não .bet.br
Contato divulgado	Sem e-mail/telefone/CNPJ corporativo; sem canal de suporte identificável

Leitura técnica. O fluxo financeiro é real e operante: o usuário deposita por PIX. O **risco não está na tecnologia nem no gateway** (instituição regular), **mas na ausência de operador identificável e de autorização**, agravada pela **divergência do recebedor do PIX**. Não há a quem cobrar prêmios/saques não pagos. A arquitetura (SPA white-label + Supabase + PIX por sub-lojista genérico em gateway de terceiro) é típica de **casas de aposta irregulares replicadas em escala**.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Apostas/cassino sem identificação do operador (sem CNPJ/razão social/endereço)	`corpo.html · mainapp.js`	ALTA
2	Sem indício de autorização federal (SPA/SIGAP); em .com, não .bet.br	`mainapp.js · RDAP`	ALTA
3	Recebedor do PIX ("KOKISCOMPRA") NÃO corresponde à marca anunciada	`pix_decode.txt`	ALTA
4	Recebe PIX e coleta dados de conta sem responsável localizável	`mainapp.js · app Supabase`	ALTA
5	Domínio recém-registrado (~11 dias), validade de 1 ano	`RDAP — 25/06/2026`	ALTA
6	Titular oculto (privacidade de registro)	`RDAP — só registrador`	MÉDIA
7	MCC 0000 (categoria de estabelecimento não especificada) no PIX	`pix_decode.txt`	MÉDIA
8	Origem/operador não revelado (Vercel anycast + Supabase serverless)	`headers.txt · dns_records.txt`	MÉDIA
9	Sem canal de contato corporativo (sem e-mail/telefone/CNPJ)	`corpo.html · mainapp.js`	MÉDIA
10	Plataforma white-label replicável (SPA + Supabase)	`mainapp.js`	BAIXA

Síntese: 5 indicadores de severidade ALTA, 4 MÉDIA e 1 BAIXA. **Nenhum fator de legitimidade** (operador identificado, autorização brasileira, contato corporativo, recebedor coerente) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 06/07/2026, conclui-se que **betouganhou.com** é uma **casa de apostas esportivas e cassino ao vivo em operação**, voltada ao público brasileiro, que recebe depósitos via PIX e coleta dados de usuários, porém **sem identificar quem a opera** (sem CNPJ, razão social ou endereço) e **sem qualquer indício de autorização** para explorar apostas/jogos no Brasil — usando **.com** em vez do padrão regulado **.bet.br**. Some-se o **registro recentíssimo (~11 dias)**, o titular oculto e, sobretudo, a **divergência do recebedor do PIX** ("KOKISCOMPRA", terceiro sem relação com a marca), coletado por meio de um gateway de terceiro (Pagsmile/Select Credit — instituição regular, a quem não se imputa conduta). Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não se cadastrar, não depositar e não fornecer dados pessoais, senha ou dados bancários** ao site.
- Desconfiar de anúncios/mensagens (Instagram, WhatsApp, Telegram, SMS) que conduzam a `betouganhou.com` ou prometam bônus/ganhos fáceis — e observar que o **PIX é cobrado por um terceiro ("KOKISCOMPRA")**, não pela marca anunciada.
- Se já houve depósito: acionar o banco e o mecanismo **MED** do PIX, reunir comprovantes/prints e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência.

Recomendações de mitigação / denúncia

- Denunciar o domínio à **Secretaria de Prêmios e Apostas (SPA/Ministério da Fazenda)** e à **Anatel** como apostas/cassino sem autorização, anexando este laudo.
- Reportar aos canais de *abuse* do registrador (**Dynadot**), da hospedagem (**Vercel**) e do back-end (**Supabase**); e comunicar ao **gateway de pagamento** (Pagsmile / Select Credit SCMEPP) a possível utilização do sub-lojista "KOKISCOMPRA" por operação de aposta irregular, para verificação de KYC/AML.

- Preservar este relatório e as evidências (com hashes SHA-256) para eventual uso administrativo ou judicial.

Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do domínio na data indicada. A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial, administrativa ou judicial. Não se imputa conduta ilícita aos provedores de infraestrutura e de pagamento citados.

— Fim do relatório —

Documento gerado por Dono do Site — OSINT & Investigação Digital · Relatório técnico baseado em dados públicos e análise de conteúdo aberto.