RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

betslots.com.br

Objeto investigado	betslots.com.br — "plataforma de apostas" que funciona como fachada/funil para o cassino win444nnbet.com
Natureza	Verificação de legitimidade, análise do fluxo de pagamento PIX e risco ao consumidor
Data da coleta	14/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise de conteúdo, BR Code PIX)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · decodificação EMV/BR Code (PIX) · exiftool
Achado central	Cassino SEM autorização federal, com licenças FABRICADAS na página "Licenças"; depósito PIX vai a recebedor genérico "BLLTDA", que não corresponde à plataforma
Classificação	**RISCO ALTO**
Emissão do laudo	14/07/2026 às 22:13

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **betslots.com.br**, realizada em **14/07/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise exclusivamente passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem interação intrusiva. Toda evidência foi preservada em arquivo no momento da coleta e teve hash SHA-256 calculado (cadeia de custódia). O solicitante forneceu ainda o código PIX "copia e cola" da tela de depósito, que foi preservado e decodificado (padrão EMV/BR Code).

O site apresenta-se como **"BETSLOTS — Sua Plataforma de Apostas Online no Brasil"**, com vitrine de slots (inclusive "Fortune Tiger", o "jogo do tigrinho") e selos de credibilidade. Tecnicamente, porém, é uma **página estática de fachada**: todos os botões de jogo e cadastro conduzem a `registration.html` → `go/login.html`, que **redireciona automaticamente** para `https://www.win444nnbet.com/?ch=162146&logo=betslots.com.br` — a plataforma de cassino real, em domínio **registrado em 24/06/2026** (cerca de 3 semanas antes da coleta), com titular oculto. O parâmetro `ch=162146` identifica um **canal de afiliado**: betslots.com.br atua como porta de entrada/captação de tráfego para uma operação de cassino terceirizada e replicável.

A página "Licenças" do site exibe **licenças fabricadas**: "Licença Principal 6GB-2024-001" atribuída à "Secretaria de Fazenda do Estado de São Paulo", "Licença de Cassino 6GB-CAS-2024-002" ao "Ministério da Economia" (pasta extinta) e "Licença de Pagamentos 6GB-PAY-2024-003" ao "Banco Central do Brasil". **Nenhum desses órgãos licencia apostas**: a exploração de apostas de quota fixa e jogos online no Brasil depende de autorização federal do Ministério da Fazenda (SPA/SIGAP, Lei 14.790/2023), e as casas autorizadas operam no domínio padronizado **.bet.br** — o que não é o caso. O domínio está registrado em nome de **pessoa física** (Maria Vitória Pereira de Souza), com contato em e-mail Gmail gratuito, **sem CNPJ ou razão social de operadora** em qualquer página.

O código PIX fornecido é **dinâmico**, gerado pelo gateway `qrcode.a55scd.com.br` (domínio da **Select Credit SCMEPP Ltda**, CNPJ 45.756.448/0001-78, instituição do grupo Transfersmile/Pagsmile). O payload assinado recuperado do gateway confirma cobrança **ATIVA de R$ 100,00** criada em 15/07/2026 (UTC). O campo "nome do recebedor" do BR Code traz apenas **"BLLTDA"** (São Paulo) — denominação genérica que **não corresponde nem a "BETSLOTS" nem a "win444nnbet"**: o depósito do apostador vai para conta de terceiro agregador, ocultando o beneficiário final.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: um site que simula credenciais regulatórias inexistentes, encaminha o usuário a um cassino de domínio recém-criado e titular oculto, e recebe depósitos PIX em nome de recebedor genérico que não corresponde ao estabelecimento, apresenta ao consumidor **risco elevado** de perda financeira e de exposição de dados. Recomenda-se **não cadastrar, não depositar e não fornecer dados** (Seções 5 e 6).

2. Metodologia e Cadeia de Custódia

Empregaram-se exclusivamente **técnicas passivas**: consultas RDAP/DNS, requisições HTTP/TLS de visitante comum, download dos scripts e imagens públicos do site, consulta a bases públicas (ipinfo.io, ip-api.com, dados cadastrais públicos da Receita Federal) e decodificação do BR Code fornecido pelo solicitante — inclusive a recuperação do payload dinâmico assinado (JWS) no endpoint público do gateway, requisição idêntica à de qualquer aplicativo bancário ao ler o QR. O DNS foi consultado via resolvedor público 1.1.1.1. As respostas foram salvas no momento da coleta e tiveram hash SHA-256 calculado. Fuso de referência: UTC, salvo indicação.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (registro.br)	`rdap_raw.json`

DNS	dig @1.1.1.1 (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_dig.txt`
Conteúdo / cabeçalhos	curl (HTTPS e porta 80)	`corpo.html · http_headers.txt · http80_headers.txt`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · ip-api.com · PTR	`ip_geo.txt`
Aplicação / fluxo	Download dos JS e páginas do funil	`main.js · registration.html · go_login.html · licencas.html · ad-*.js`
Plataforma de destino	RDAP (Verisign) + HTTP	`rdap_win444nnbet.json · win444_home.html`
PIX (BR Code)	Decodificação TLV/EMV + payload dinâmico (JWS)	`pix_copiaecola.txt · pix_decodificado.txt · pix_payload_jws.txt`
Gateway do PIX	RDAP (registro.br) + cadastro público do CNPJ	`rdap_a55scd.json · cnpj_selectcredit.json`
Imagens / metadados	Download de assets · exiftool -a -G1 -s	`imagens/ · metadata_exiftool.txt`

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

Domínio	betslots.com.br (ccTLD .br — registro.br)
Registro	30/12/2024 · última alteração 01/12/2025 · expira 30/12/2026
Titular	**Maria Vitória Pereira de Souza — pessoa física** · CPF ***.044.814-** (mascarado pelo registro.br) · **sem CNPJ**
Contato técnico	mesmo nome · e-mail `keenocost@gmail.com` (Gmail gratuito)
Servidores de nome	ns-1155.awsdns-16.org e outros três — **AWS Route 53**
DNS — A	18.155.21.16 / .54 / .91 / .121 (Amazon CloudFront) · www → du5w7e6hgak09.cloudfront.net · sem MX · TXT só google-site-verification
Hospedagem (borda)	AS16509 Amazon.com — **CloudFront** (PTR *.gru3.r.cloudfront.net, POP São Paulo) · origem `nginx` oculta atrás do CDN
Conteúdo estático	Last-Modified: 02/10/2025 — landing publicada e não alterada desde então
Certificado TLS	CN=betslots.com.br · emissor Amazon RSA 2048 M03 (DV, via AWS Certificate Manager) · válido 08/09/2025–07/10/2026 · SAN: betslots.com.br, www
Fingerprint SHA-256	87:CF:7B:EA:F5:E2:0D:72:2F:B3:9C:D8:5F:3D:70:CF:DC:85:72:6B:15:58:63:FB:FA:76:01:23:B6:D9:E1:71
Plataforma de destino	**win444nnbet.com** — registrado **24/06/2026** (Amazon Registrar), titular oculto, NS AWS Route 53; casca JavaScript sem título
Gateway do PIX	**a55scd.com.br** — Select Credit SCMEPP Ltda, CNPJ 45.756.448/0001-78 (ativa, São Paulo/SP; sócia Transfersmile Holding Financeira — grupo Pagsmile) · NS Cloudflare

Leitura técnica. A fachada betslots.com.br tem 18 meses de registro, mas está em nome de **pessoa física com e-mail gratuito** — incompatível com uma "plataforma de apostas" empresarial. Toda a infraestrutura (DNS, CDN, TLS) é da AWS; o CloudFront oculta o servidor de origem. O certificado DV da Amazon comprova apenas o controle do domínio, **não a identidade de empresa**. O cassino de destino, win444nnbet.com, tem **3 semanas de existência** e titular oculto. Não se imputa conduta à Amazon/AWS, ao registro.br, à Cloudflare nem à Select Credit/Pagsmile, provedores de infraestrutura e de pagamento.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Funil. A landing exibe vitrine de jogos e botões de cadastro que apontam para `registration.html`; dela, `go/login.html` redireciona de imediato (meta-refresh + `location.replace`) para `win444nnbet.com/?ch=162146&logo=betslots.com.br`, onde ocorrem de fato o cadastro, o depósito e o jogo. A landing carrega ainda um **kit de scripts de terceiros** (`image.app366.link`, consumindo `api.share-us.org`) que injeta comentários de "ganhadores" e botões de compartilhamento (TikTok, Kwai, Instagram) — artefatos típicos de **kits replicáveis de cassino falso** —, além de contador StatCounter (projeto 13202996) para medir o tráfego captado. Não há qualquer formulário local: os dados pessoais e financeiros são entregues diretamente à plataforma de destino.

Decodificação do PIX "copia e cola" (EMV/BR Code)

Campo	Constatação
Tipo de cobrança	Dinâmica (Point of Initiation = 12) · CRC16 válido (5326)
URL do payload (campo 26)	`qrcode.a55scd.com.br/v1/7be9dc5a-a9e5-46d4-9b96-216d2661ec90`
Recebedor (campo 59)	**"BLLTDA"** — denominação genérica/truncada, sem correspondência com BETSLOTS ou win444nnbet
Cidade (60) / MCC (52)	SAOPAULO · MCC 0000 (não categorizado) · moeda 986 (BRL)
Payload dinâmico (JWS)	Cobrança **ATIVA** de **R$ 100,00** · txid su8VqIEdDi9czUAONRigkxw7zH · chave PIX e8a77e65-e226-4415-821d-25c5afd542b2 · criada 15/07/2026 00:40 UTC · validade 24 h · assinatura PS256 do gateway
Gateway / intermediário	a55scd.com.br — Select Credit SCMEPP Ltda (CNPJ 45.756.448/0001-78, ativa; grupo Transfersmile/Pagsmile). Instituição de crédito registrada — o recebedor é **cliente** do gateway, não o gateway em si
Correspondência loja × recebedor	**NÃO HÁ** — o depósito vai a conta agregadora de terceiro; o beneficiário final não é identificável publicamente

Leitura técnica. O fluxo financeiro é real e operante: a cobrança estava ATIVA no gateway no momento da coleta. O apostador acredita depositar na "BETSLOTS", mas o BR Code paga um recebedor genérico ("BLLTDA") por meio de um agregador de pagamentos, **quebrando o vínculo entre a marca anunciada e o destino do dinheiro** — padrão recorrente em cassinos irregulares para dificultar rastreio e contestação. A página "Licenças" fabricada (números "6GB-…" atribuídos a Secretaria de Fazenda-SP, Ministério da Economia, Banco Central e Inmetro — órgãos que não licenciam apostas) reforça a intenção de simular legitimidade. As imagens da vitrine usam marcas de jogos de terceiros (PG Soft: "Fortune Tiger", "Fortune Rabbit", "Fortune Snake") sem indício de autorização — ver relatório complementar de imagens.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Cassino/apostas voltado ao Brasil sem autorização federal (SPA/SIGAP); domínio comum, não .bet.br	`corpo.html` · `licencas.html` · `RDAP`	ALTA
2	Página "Licenças" com licenças FABRICADAS, atribuídas a órgãos que não licenciam apostas	`licencas.html`	ALTA
3	Fachada/funil de afiliado (ch=162146) para cassino em domínio registrado 20 dias antes da coleta, titular oculto	`go_login.html` · `rdap_win444nnbet.json`	ALTA
4	Recebedor do PIX genérico ("BLLTDA") sem correspondência com o estabelecimento; beneficiário final oculto por agregador	`pix_decodificado.txt` · `pix_payload_jws.txt`	ALTA
5	Domínio em nome de pessoa física com e-mail Gmail; nenhum CNPJ/razão social de operadora no site	`rdap_raw.json` · `corpo.html`	ALTA
6	Kit de scripts de terceiros que injeta comentários de "ganhadores" e compartilhamento (padrão de cassino falso replicável)	`ad-comment.js` · `ad-plugin.js`	MÉDIA

7	Imagens de jogos com marcas de terceiros (PG Soft), metadados removidos, extensões trocadas e nomes de template	`imagens/ · metadata_exiftool.txt`	MÉDIA
8	Origem oculta atrás de CloudFront; landing estática sem atualização desde 02/10/2025	`http_headers.txt · ip_geo.txt`	MÉDIA
9	Links de redes sociais genéricos (/BETSLOTS) sem perfil verificável	`corpo.html`	BAIXA
10	Rastreador StatCounter para medição de tráfego captado (compatível com campanhas de captação)	`go_login.html`	BAIXA

Síntese: 5 indicadores de severidade ALTA, 3 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (operador identificado, autorização federal, canal corporativo, correspondência entre marca e recebedor do pagamento) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 14/07/2026, conclui-se que **betslots.com.br** é a **fachada brasileira de um cassino online irregular**: apresenta-se como plataforma própria ("BETSLOTS"), exibe **licenças fabricadas** em nome de órgãos que não licenciam apostas, e encaminha todo o tráfego, via canal de afiliado, para **win444nnbet.com** — domínio de 3 semanas, titular oculto, sem autorização SPA/SIGAP e fora do padrão .bet.br. O depósito por PIX, comprovado por cobrança ATIVA de R$ 100,00 no gateway, é creditado a recebedor genérico **"BLLTDA"**, sem correspondência com a marca anunciada, por meio de agregador que oculta o beneficiário final. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não se cadastrar, não depositar e não fornecer CPF, senha ou dados bancários** em betslots.com.br ou win444nnbet.com.
- Se já houve depósito: acionar imediatamente o banco e o mecanismo **MED** do PIX (Banco Central), informando o txid `su8VqIEdDi9czUAONRigkxw7zH` e a chave do recebedor; reunir comprovantes; registrar Boletim de Ocorrência e reclamação em **consumidor.gov.br**.
- Desconfiar de anúncios e mensagens (Instagram, TikTok, Kwai, WhatsApp) que conduzam a "BETSLOTS" ou prometam bônus/ganhos fáceis no "jogo do tigrinho".

Recomendações de mitigação / denúncia

- Denunciar betslots.com.br e win444nnbet.com à **Secretaria de Prêmios e Apostas (SPA/Ministério da Fazenda — SIGAP)** e à **Anatel**, como exploração de apostas sem autorização (passível de bloqueio), anexando este laudo.
- Reportar aos canais de **abuse da Amazon/AWS** (CloudFront, Route 53 e Amazon Registrar hospedam a fachada e o cassino) e ao **registro.br** (titularidade de pessoa física para operação de apostas).
- Comunicar o recebedor "BLLTDA" ao **compliance da Select Credit/Pagsmile** (gateway a55scd.com.br) e ao Banco Central, para verificação do cliente e eventual encerramento da chave PIX.
- Comunicar a **PG Soft** (titular das marcas "Fortune Tiger/Rabbit/Snake") o uso não autorizado de suas marcas e artes.

Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado dos sistemas 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 (Amazon/AWS, Cloudflare, registro.br, Select Credit/Pagsmile), meros intermediários.

— Fim do relatório —

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