RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

estelaroficial.bet

Objeto investigado	estelaroficial.bet - site de apostas e cassino online que se anuncia como "Oficialmente Legalizada!" (gTLD .bet)
Natureza	Verificação de legitimidade regulatória e de risco ao apostador
Data da coleta	02/09/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise do código da página)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do HTML e dos scripts
Achado central	Mesmo modelo técnico de **bmwbet.site** - scripts, chave de biblioteca e textos idênticos -, com o mesmo fluxo de **"taxa de saque" de R$ 30,00 por Pix**, em domínio `.bet` que não é o `.bet.br` exigido no Brasil
Classificação	**RISCO ALTO**
Emissão do laudo	02/09/2026 as 22:14

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **estelaroficial.bet**, realizada em **02/09/2026** 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 envio de dados pessoais e sem qualquer depósito ou aposta. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio **está no ar**, atrás da Cloudflare, e entrega um site de apostas e cassino online intitulado **"Estelar Oficial - Oficialmente Legalizada! - Bem vindo!"**, com a chamada "Jogue agora e receba bônus diários!", catálogo de *slots* (Fortune Dragon, Fortune Tiger, Fortune Ox, Fortune Mouse, Fortune Rabbit, Fortune Snake), roletas, "cassino ao vivo" e programa de indicação. O acesso direto pelo nome falhou no resolvedor local durante a coleta; o conteúdo foi obtido apontando a requisição ao endereço IP publicado no DNS autoritativo da Cloudflare.

O achado central é o mesmo de **bmwbet.site**, e os dois sites **compartilham o mesmo modelo**. As evidências de vínculo técnico são objetivas e verificáveis lado a lado: a **mesma chave de biblioteca Font Awesome** (`kit.fontawesome.com/6728d0711b.js`), os **mesmos quatro scripts próprios** (`cmsfilter.js`, `cmssort.js`, `cmsload.js`, `scrolldisable.js`), os **mesmos domínios de ativos externos** (`jogue.com`, `static.7k.bet.br`, `assets.website-files.com`, `vectorflags.s3.amazonaws.com`), o mesmo rodapé **"© 2023"** e a **mesma frase de marketing** "Oficialmente Legalizada!". Não se trata de dois sites parecidos: é o **mesmo produto** publicado sob marcas diferentes.

E, como em **bmwbet.site**, o HTML entregue ao visitante já traz em texto fixo todo o fluxo de um **saque condicionado ao pagamento antecipado de uma taxa**: "Realize o seu saque", "VOCÊ NÃO TEM O VALOR MÍNIMO NECESSÁRIO NA CARTEIRA PARA SAQUE (R$ 50)", **"de acordo com as regulamentações, será deduzida uma taxa de R$ 30,00 sobre todos os ganhos com apostas ao efetuar o saque"** e a tela de **QR Code Pix** com "Após o pagamento da taxa, o valor descontado dos impostos será transferido imediatamente através do PIX". Nenhuma regulamentação brasileira exige que o apostador transfira dinheiro ao operador para receber um prêmio: tributos sobre premiação são retidos na fonte.

Quanto à legalidade alegada, vale a mesma constatação. O domínio usa o gTLD genérico `.bet`, que **não se confunde** com o `.bet.br` obrigatório para operadores autorizados pelo Ministério da Fazenda no Brasil. O registro é de **09/02/2026**, com **titular oculto** no RDAP e DNS delegado à Cloudflare, que oculta o endereço real da hospedagem. A página ainda referencia o domínio irmão `nacionaloficial.bet`, indicando que a rede vai além dos dois casos aqui documentados.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: um site de apostas com titular oculto, que se declara "Oficialmente Legalizada" fora do domínio `.bet.br` exigido no Brasil, tecnicamente idêntico a **bmwbet.site** e com a mesma cobrança de **taxa de R$ 30,00 por Pix para liberar saque**, oferece **risco elevado**. Recomenda-se **não depositar, não se cadastrar e jamais pagar qualquer taxa para sacar** (Seções 5 e 6).

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 (.bet - registrador Hostinger)	`rdap_raw.json`

DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS com resolução dirigida ao IP publicado	`corpo_retry.html` · `headers_retry.txt`
Comparação de modelo	Confronto de scripts, chaves e textos com bmwbet.site	`corpo_retry.html` · `corpo_home.html`
Geolocalização do IP	ipinfo.io · PTR reverso	`geoip.json`
Consolidação	Extração de fatos e hashes SHA-256	`hash_manifest.txt`

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

Domínio	estelaroficial.bet (gTLD .bet - **não** é o ccTLD regulado .bet.br)
Registro	**09/02/2026** · expira 09/02/2027 · última alteração 12/08/2026
Idade na coleta	Cerca de **7 meses**
Titular	**Oculto** (o RDAP expõe apenas o registrador)
Registrador	HOSTINGER operations, UAB (IANA 1636) · abuse@hostinger.com
Status	clientTransferProhibited
Servidores de nome	crystal.ns.cloudflare.com · jaxson.ns.cloudflare.com
DNS - A	104.21.40.190 · 172.67.156.79 (+ AAAA) · **sem MX** · **sem TXT**
Hospedagem	AS13335 Cloudflare, Inc. - **origem real oculta** pelo proxy
Resolução no acesso	O nome **não resolveu** no resolvedor local durante a coleta; conteúdo obtido via IP autoritativo
Domínio irmão citado	`nacionaloficial.bet` referenciado na própria página
Domínio regulado?	**Não** - operadores autorizados no Brasil usam `.bet.br`

Leitura técnica. Titular oculto, ausência de e-mail próprio (sem MX) e proxy da Cloudflare diante da origem compõem um perfil de **baixa rastreabilidade do responsável**. O gTLD `.bet` é aberto e pode ser registrado por qualquer pessoa em qualquer país - a semelhança visual com o `.bet.br` brasileiro, este sim restrito a operadores autorizados, é um fator de confusão relevante para o consumidor. Não se imputa conduta à Hostinger nem à Cloudflare, meras provedoras de registro e de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é uma **plataforma de apostas e cassino online** construída sobre o mesmo modelo pronto identificado em **bmwbet.site**. O visitante encontra login/cadastro, botão "PIX", "Depositar", "TORNAR-SE VIP", catálogo de *slots*, roletas, "cassino ao vivo", suporte e um programa "Indique e Ganhe". Todo o fluxo de depósito e de saque é interno ao site.

Elemento comparado	estelaroficial.bet e bmwbet.site
Chave Font Awesome	`kit.fontawesome.com/6728d0711b.js` - **idêntica** nos dois
Scripts próprios	`cmsfilter.js` · `cmssort.js` · `cmsload.js` · `scrolldisable.js` - **mesmo conjunto**
Ativos externos	`jogue.com` · `static.7k.bet.br` · `assets.website-files.com` · `vectorflags.s3.amazonaws.com`
Frase de marketing	"Oficialmente Legalizada!" - **idêntica**
Fluxo de saque	Piso de R$ 50 + **taxa de R$ 30,00 por Pix** - **texto idêntico**
Rodapé	**"© 2023"** nos dois sites
Registrador	HOSTINGER operations, UAB nos dois domínios

Aspecto	Constatação
Tipo de site	Casa de apostas / cassino online voltada ao público brasileiro (conteúdo em PT-BR, Pix, reais)
Alegação de legalidade	**"Oficialmente Legalizada!"** no `og:title`, no `twitter:title` e no rodapé
Domínio	**.bet** (gTLD aberto) - **não** é o `.bet.br` exigido no Brasil
Taxa para sacar	**R$ 30,00 por Pix antes da liberação do saque**, com QR Code, fixo no HTML
Piso de saque	R$ 50,00 mínimos em carteira antes de qualquer pedido
Meio de pagamento	**Pix**, gerado dentro do próprio site - beneficiário não exposto ao visitante
Vínculo com bmwbet.site	**Mesmo modelo**: chave de biblioteca, scripts, ativos, textos e rodapé idênticos
Rede	A página referencia `nacionaloficial.bet` - indício de mais domínios irmãos
Ativos de terceiros	Arquivos carregados de `static.7k.bet.br` (operador regulado) e `jogue.com`
Identificação do operador	**Inexistente** - sem CNPJ, razão social, endereço ou e-mail de contato

Leitura técnica. A tabela acima é o núcleo probatório do vínculo entre os dois domínios. Uma **chave de kit Font Awesome** é um identificador único emitido para uma conta específica; encontrá-la idêntica em dois sites de marcas diferentes indica **o mesmo responsável técnico ou o mesmo fornecedor do modelo**. Somada ao conjunto idêntico de scripts próprios, aos mesmos domínios de ativos e aos textos literalmente iguais - inclusive o valor de R$ 30,00 e o rodapé "© 2023" -, a coincidência deixa de ser plausível por acaso. Quanto ao risco ao consumidor, vale a mesma leitura de **bmwbet.site**: exigir um **Pix de entrada** para liberar um saque inverte o fluxo de dinheiro e é o mecanismo pelo qual o prejuízo se realiza mesmo para quem "ganhou". A coleta foi passiva: nenhum cadastro, depósito ou código Pix foi gerado.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Fluxo de "taxa de saque" de R$ 30,00 por Pix, com QR Code, fixo no código da página	`corpo_retry.html`	ALTA
2	Alegação "Oficialmente Legalizada!" sem domínio .bet.br exigido da operação autorizada no Brasil	`corpo_retry.html`	ALTA

3	Modelo técnico idêntico ao de bmwbet.site (mesma chave Font Awesome, scripts, ativos e textos)	`corpo_retry.html`	ALTA
4	Nenhuma identificação do operador: sem CNPJ, razão social, endereço ou e-mail	`corpo_retry.html` · `dns_records.txt`	ALTA
5	Titular oculto no RDAP e origem mascarada por proxy da Cloudflare	`rdap_raw.json` · `geoip.json`	ALTA
6	Uso do gTLD .bet, visualmente confundível com o .bet.br regulado brasileiro	`rdap_raw.json`	MEDIA
7	Referência ao domínio irmão nacionaloficial.bet - rede com mais endereços	`corpo_retry.html`	MEDIA
8	Piso artificial de R$ 50 em carteira antes de qualquer pedido de saque	`corpo_retry.html`	MEDIA
9	Carregamento de ativos de static.7k.bet.br, domínio de operador regulado	`corpo_retry.html`	BAIXA
10	Rodapé "© 2023" e ausência total de MX/TXT no domínio	`corpo_retry.html` · `dns_records.txt`	BAIXA

Síntese: 5 indicadores de severidade ALTA, 3 MEDIA e 2 BAIXA. **Nenhum fator de legitimidade** (domínio `.bet.br`, autorização federal verificável, CNPJ, identificação do operador) foi constatado. O caso deve ser lido em conjunto com o laudo de **bmwbet.site**.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **02/09/2026**, conclui-se que **estelaroficial.bet** apresenta **risco alto ao apostador**. O site oferece apostas e cassino online ao público brasileiro declarando-se "Oficialmente Legalizada", mas opera em gTLD `.bet` - e não no `.bet.br` exigido de operadores autorizados no Brasil -, tem **titular oculto**, origem mascarada por proxy e **não identifica qualquer pessoa física ou jurídica responsável**. O código da página traz o mesmo fluxo pronto de **cobrança de R$ 30,00 por Pix como condição para liberar o saque** documentado em **bmwbet.site**. A identidade do modelo técnico entre os dois domínios - mesma chave de biblioteca, mesmos scripts, mesmos ativos externos, mesmos textos e mesmo rodapé - demonstra que não se trata de casos isolados, mas de **uma mesma operação replicada sob marcas distintas**, com ao menos um terceiro endereço (`nacionaloficial.bet`) citado na própria página. Classifica-se o caso como **RISCO ALTO**.

Recomendações ao consumidor / solicitante

- **Não depositar, não se cadastrar e não fornecer CPF, documentos ou dados bancários** ao site.
- **Jamais pagar qualquer "taxa", "imposto" ou "liberação" para sacar**: em operação legítima, tributos são retidos na fonte e descontados do prêmio - o dinheiro nunca vai do apostador para a casa a fim de liberar um saque.
- Conferir se a casa opera sob domínio `.bet.br` e consultar a lista oficial de operadores autorizados publicada pelo **Ministério da Fazenda / Secretaria de Prêmios e Apostas** antes de qualquer depósito.
- Atenção à confusão entre `.bet` (gTLD aberto, qualquer um registra) e `.bet.br` (restrito a operadores autorizados no Brasil).
- Se já houve pagamento: acionar o banco e o mecanismo **MED** do Pix imediatamente, reunir comprovantes e registrar Boletim de Ocorrência e reclamação em **consumidor.gov.br**.

Recomendações de mitigação / denúncia

- Denunciar o domínio ao canal de abuse do registrador (`abuse@hostinger.com`) e à Cloudflare, anexando este laudo e o laudo de **bmwbet.site**, que documenta o mesmo modelo.

- Comunicar a **Secretaria de Prêmios e Apostas (SPA/MF)** a oferta de apostas ao público brasileiro fora do regime autorizado, indicando os dois domínios e o terceiro citado na página.
- Informar o operador de `7k.bet.br` sobre o carregamento de seus ativos por este site, para as medidas de proteção de marca que entender cabíveis.
- Preservar este relatório e as evidências (pasta `evidencias/`, 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 (coleta em 02/09/2026). A classificação expressa um **juízo técnico de risco** e não substitui decisão de autoridade policial, administrativa, regulatória ou judicial. A identidade de modelo técnico com **bmwbet.site** demonstra origem comum do **código**; a identificação das pessoas por trás de cada domínio não é possível apenas por fontes abertas e não é aqui afirmada. Não se imputa conduta ilícita aos provedores de infraestrutura citados (Hostinger, Cloudflare), nem ao operador de `7k.bet.br`, cujos ativos aparecem carregados pelo site investigado sem que se possa afirmar qualquer vínculo entre eles.*

Anexo A - Manifesto de Integridade (SHA-256)

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

Arquivo	SHA-256
`corpo_home.html (0 bytes)`	`e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`
`dns_records.txt (413 bytes)`	`58ac014738d355f51aad68e997c5bf3057a16ad7e4250605ba5453d427f42965`
`geoip.json (288 bytes)`	`ff19dfe4fe70ed078ae5a17d107e8b57e1a6939e0828f81c5dae9abf1b62dd28`
`headers_home.txt (0 bytes)`	`e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`
`rdap_raw.json (7640 bytes)`	`13368e68b65f1535d1a7967217387d8eeafc9fd82ae4f1f49b1e9725f27f84d5`
`tls_cert.txt (67 bytes)`	`fd4601dcf3b285b522c6d9ff265c3abdaa04536ae1abbe191f0a02a66956b40a`

- Fim do relatório -