RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

bet2m.bet

Objeto investigado	bet2m.bet — plataforma de apostas/cassino online (gTLD .bet)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	08/06/2026 (RDAP, DNS, HTTP/TLS, geolocalização, crt.sh)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo e do app
Achado central	Site de apostas SEM identificação de operador e SEM autorização (Brasil)
Classificação	**RISCO ALTO**
Emissão do laudo	08/06/2026 às 12:52

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **bet2m.bet**, realizada em **08/06/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem qualquer interação intrusiva ou exploração de vulnerabilidade. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio **está no ar** e entrega uma **plataforma de apostas/cassino online em português** (título "BET2M", aplicação Laravel sobre nginx), com cadastro de usuários, carteira, apostas esportivas, sistema de afiliados/indicação e **depósito via PIX** intermediado pelo gateway **SuitPay**. O cadastro coleta **CPF, e-mail, telefone e senha**. O conjunto de sinais é, porém, o de uma operação **opaca e sem lastro verificável**: domínio **recém-registrado** (13/04/2026), **titular oculto**, e — no próprio site — **nenhuma identificação do operador** (sem CNPJ, razão social ou endereço), **nenhum selo de autorização regulatória** e, como único contato, um **e-mail gratuito do Gmail** (CLUBE777@gmail.com).

Ponto juridicamente relevante: no Brasil, a exploração de apostas de quota fixa ("bets") depende 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 **.bet** (genérico) e **não apresenta qualquer indício de autorização** — perfil compatível com **operação irregular/não autorizada**, categoria sujeita a bloqueio pelas autoridades brasileiras.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: uma plataforma que recebe dinheiro (PIX) e dados sensíveis (CPF) **sem identificar quem a opera nem comprovar autorização** oferece ao consumidor **risco elevado** — ausência de responsável localizável, ausência de garantia de pagamento de prêmios e exposição de dados pessoais. 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**. 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; como o cliente curl não conduziu o corpo nas portas 443/80, o conteúdo HTTPS, o aplicativo JavaScript e o certificado foram coletados por requisição HTTP/1.1 bruta sobre TLS via `openssl s_client` — procedimento estritamente passivo. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Identity Digital / .bet)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Conteúdo / app	openssl s_client (HTTP/1.1 sobre TLS)	`corpo_https.html · app_js_raw.txt`
Certificado TLS	openssl s_client / x509	`ssl_cert.txt · ssl_raw.txt`
Geolocalização do IP	ipinfo.io · ip-api.com · PTR	`ipinfo_*.json · ipapi_*.json · ptr_reverse.txt`
Intermediário de pagto.	RDAP registro.br (suitpay.com.br)	`rdap_suitpay.json`
Certificados (CT) / histórico	crt.sh · Internet Archive (CDX)	`crtsh.json · wayback_cdx.json`

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

Domínio	bet2m.bet (gTLD .bet — Identity Digital)

Registro	**13/04/2026** · expira 13/04/2027 (validade de 1 ano)
Idade na coleta	**~8 semanas** — domínio recente
Titular	**Oculto** (privacidade de gTLD; RDAP expõe só o registrador)
Registrador	HOSTINGER operations, UAB
Servidores de nome	athena / apollo.dns-parking.com (parking Hostinger)
DNS — A	216.238.126.188 · sem AAAA, sem MX, sem TXT/SPF
www	aponta para o mesmo IP (216.238.126.188)
Hospedagem	AS20473 The Constant Company (Vultr)
Geolocalização do IP	Osasco / São Paulo — Brasil (datacenter; hosting: true)
PTR reverso	216-238-126-188.constant.com
Servidor web	nginx/1.18.0 (Ubuntu) · aplicação Laravel
Certificado TLS	CN=bet2m.bet · emissor Let's Encrypt (DV) · válido 06/06/2026–04/09/2026
Série / Fingerprint	05EC196D…3358 · SHA-256 A4:6D:18:63:F1:61:2B:CE:65:5B:40:3A:EB:17:4C:6A…
Histórico (crt.sh)	3 emissões Let's Encrypt desde 13/04/2026 (1ª no dia do registro) — só o apex

Leitura técnica. Registro recente, validade de 1 ano e titular oculto compõem um perfil de **baixa rastreabilidade do responsável**. O certificado DV gratuito (Let's Encrypt) comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. Não se imputa conduta ao registrador (Hostinger) nem ao provedor de hospedagem (Vultr), meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site entrega uma **plataforma funcional de apostas/cassino** em português (pt-BR), com área de cadastro/login, carteira (`/profile/wallet`), apostas esportivas, promoções e um **programa de afiliados/indicação** (`/profile/linkconvite` e `/profile/comissao`). O depósito é feito por **PIX**, processado pelo gateway **SuitPay** (endpoint `/api/suitpay/check-payment` identificado no código).

Aspecto	Constatação
Tipo de serviço	Apostas esportivas e cassino online (plataforma "BET2M")
Meio de pagamento	Depósito via PIX
Intermediário (gateway)	SuitPay — Suit Business Ltda, CNPJ 38.333.425/0001-95 (RDAP registro.br)
Dados pessoais coletados	CPF, e-mail, telefone e senha (cadastro)
Identificação do operador	**Ausente** — sem CNPJ, razão social ou endereço no site
Autorização / licença	**Ausente** — sem selo SPA/SIGAP, sem "jogo responsável", sem 18+
Domínio	.bet (genérico) — **não** o padrão .bet.br exigido das casas autorizadas no Brasil
Contato divulgado	CLUBE777@gmail.com (e-mail gratuito) · sem canal corporativo

Leitura técnica. O fluxo financeiro é real e operante: o usuário deposita por PIX e fornece CPF. O **risco não está na tecnologia, mas na ausência de responsável identificável e de autorização**: não há a quem cobrar prêmios não pagos, nem garantia de tratamento adequado dos dados (CPF/senha). A presença do gateway SuitPay (intermediário regular, CNPJ ativo) **não confere legitimidade ao site** — o gateway apenas processa o PIX; não se imputa a ele conduta do operador do site. Caso seja fornecida captura da tela de pagamento (pasta `pix/`), o laudo pode ser complementado com a decodificação do BR Code (EMV) e a checagem do recebedor.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Casa de apostas sem identificação do operador (CNPJ/razão social/endereço)	`corpo_https.html`	ALTA
2	Sem indício de autorização federal (SPA/SIGAP) e em .bet, não .bet.br	`corpo_https.html` · RDAP	ALTA
3	Recebe PIX e coleta CPF/senha sem responsável localizável	`app_js_raw.txt`	ALTA
4	Domínio recém-registrado (~8 semanas), validade de 1 ano	`RDAP — 13/04/2026`	MÉDIA
5	Titular oculto (privacidade de gTLD)	`RDAP — só registrador`	MÉDIA
6	Programa de afiliados/indicação com comissão	`app_js_raw.txt`	MÉDIA
7	Único contato é e-mail gratuito (Gmail)	`corpo_https.html`	BAIXA
8	Sem e-mail próprio (MX/TXT) e domínio em parking	`dns_records.txt`	BAIXA

Síntese: 3 indicadores de severidade ALTA, 3 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (operador identificado, autorização, contato corporativo, histórico) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 08/06/2026, conclui-se que **bet2m.bet** é uma **plataforma de apostas/cassino online em operação**, que recebe depósitos via PIX e coleta dados pessoais (CPF, senha), porém **sem identificar quem a opera** e **sem qualquer indício de autorização** para explorar apostas no Brasil — usando domínio **.bet** em vez do padrão regulado **.bet.br**. Soma-se a isso o registro recente, o titular oculto e o contato limitado a um e-mail gratuito. 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 pessoais** ao site.
- Desconfiar de anúncios e mensagens (Instagram, WhatsApp, Telegram, SMS) que conduzam a `bet2m.bet` ou prometam bônus/ganhos fáceis.
- Se já houve depósito: acionar o banco e o mecanismo **MED** do PIX, reunir comprovantes 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 casa de apostas sem autorização, e reportar aos canais de abuse do registrador (Hostinger) e da hospedagem (Vultr), anexando este laudo.
- 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. 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.

Anexo A — Manifesto de Integridade das Evidências

Os arquivos abaixo foram preservados na subpasta `evidencias/` e seus resumos criptográficos (SHA-256) calculados no momento da coleta. Qualquer alteração posterior modifica o hash, permitindo a detecção. Verificação: `sha256sum -c hash_manifest.txt` (dentro de evidencias/).

Arquivo	SHA-256
app_js_raw.txt	fdbd80eb5f90789664a07d5813a20f704e624af2926818bccf501f643df0979d
coleta_notas.txt	8deb4dbf6bc8f261964ab1474128976b1229276e7a359c4fddbe77d928511866
corpo_https.html	bad133bedebddc33072b383ee31cf3c68c14df816fd6a0e3c4e535e58bf9e9aa
crtsh.json	d16028cb078008ac4a421c6145c556a0165705faeb746cb41077639ec3e3d6b7
dns_records.txt	d859c57ecbabf9aefb1158da5d2ae71d90b2fbf1e47b1662494a2a1d3d80c3b6
ipapi_216.238.126.188.json	ed56389091bfd71ee3feae69a52b8cde2dae2d8d2a0c273b85976b4e8658c2a9
ipinfo_216.238.126.188.json	efa3e4cd9ccfbf78a2f0f2a2968a4e4444c3bdfdf6c194e1c80b4ecee1a391b9
ptr_reverse.txt	44ac192c70e553ed4413269d29fd9a6f1f18b70c9f89dca1190025f240e6fbfe
raw_response.txt	bad133bedebddc33072b383ee31cf3c68c14df816fd6a0e3c4e535e58bf9e9aa
rdap_raw.json	c7e1bfd2ca68b873c43347ab9ff89b0036963e81973e935824a68924b08d6a7d
rdap_suitpay.json	f357a56c48ebe57a1af92340352a6792e530a43536c571df2a3fd7604c9e2481
ssl_cert.txt	2a35e3a2ca52db6a64b3ddd530fe5fd911e103f7d25cd62e0aba20a7194eea23
ssl_raw.txt	7f429aeb694f82845f9036a7d312edcf9e575602c42309e72570399389f33f4f
wayback_cdx.json	37517e5f3dc66819f61f5a7bb8ace1921282415f10551d2defa5c3eb0985b570

— Fim do relatório —

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