RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

7play77.com

Objeto investigado	7play77.com — cassino online de slots / apostas (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	10/06/2026 (RDAP, DNS, HTTP/TLS, geolocalização, crt.sh, análise do app)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo e do app
Achado central	Cassino online SEM identificação de operador e SEM autorização (Brasil)
Classificação	**RISCO ALTO**
Emissão do laudo	10/06/2026 às 21:50

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **7play77.com**, realizada em **10/06/2026** 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 um **cassino online de "slots" / apostas em português** (título "7PLAY77.COM | Casino Online de Slots Premiados"), construído como aplicação de página única (SPA Vue) servida atrás da **Cloudflare**. O front-end consome uma **API hospedada em domínio separado** (`g.adbet77.com`, sobre AWS em São Paulo), com cadastro de usuários, carteira, depósito e **saque via PIX** (`/pay/v1/payInOrder` e `payOutOrder`), bônus de depósito e um **programa de afiliados/indicação** multinível. O cadastro coleta **CPF, nome, e-mail, telefone, senha** e **dados bancários** (banco/conta) para saque.

O conjunto de sinais é o de uma operação **opaca e sem lastro verificável**: domínio **recém-registrado** (06/05/2026), **titular oculto**, infraestrutura de origem **mascarada por Cloudflare**, e — no próprio site — **nenhuma identificação do operador** (sem CNPJ real, razão social ou endereço; o único "CNPJ" presente no código é o placeholder de template `00.000.000/0000-00`), **nenhum selo de autorização regulatória brasileira** e suporte limitado a um canal de **Telegram**. O código exibe ainda uma alegação genérica e não verificável de "licença de jogos dos EUA".

Ponto juridicamente relevante: no Brasil, a exploração de apostas de quota fixa e jogos de azar online ("bets"/cassino) 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 **.com** genérico, **não apresenta qualquer indício de autorização** e tem como público-alvo declarado o Brasil (idioma pt-BR, moeda BRL, coleta de CPF, PIX) — 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, senha, dados bancários) **sem identificar quem a opera nem comprovar autorização** oferece ao consumidor **risco elevado** — ausência de responsável localizável, ausência de garantia de pagamento de prêmios/saques 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 HTTP atrás da Cloudflare, o conteúdo HTTPS, o aplicativo JavaScript e os cabeçalhos 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 (Verisign / .com — registrador Gandi)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Conteúdo / cabeçalhos	openssl s_client (HTTP/1.1 sobre TLS)	`corpo_https.html` · `headers_https.txt` · `raw_https_response.txt`
Aplicação (front-end)	Download dos bundles JS do site	`app_main_js.js` · `app_env_js.js`
Certificado TLS	openssl s_client / x509	`ssl_cert.txt` · `ssl_raw.txt`

Geolocalização do IP	ipinfo.io · ip-api.com	`ipinfo_*.json · ipapi_*.json`
Backend de API	RDAP + DNS (adbet77.com / g.adbet77.com)	`rdap_adbet77.json · dns_backend_adbet77.txt`
Certificados (CT)	crt.sh	`crtsh.json`
Imagens / metadados	Download de assets · exiftool	`imagens/ · metadata_exiftool.txt`

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

Domínio	7play77.com (gTLD .com — Verisign)
Registro	**06/05/2026** · expira 06/05/2027 (validade de 1 ano)
Idade na coleta	**~5 semanas** — domínio recente
Titular	**Oculto** (privacidade; RDAP expõe só o registrador)
Registrador	Gandi SAS
Status	clientTransferProhibited
Servidores de nome	jarred / lauryn.ns.cloudflare.com (Cloudflare)
DNS — A	104.21.2.110 · 172.67.129.27 (Cloudflare) · AAAA presente · sem MX · sem TXT/SPF
www	aponta para os mesmos IPs Cloudflare
Hospedagem (borda)	AS13335 Cloudflare, Inc. — **proxy/CDN que oculta o IP de origem**
Geolocalização do IP	Anycast Cloudflare (não revela a localização do servidor real)
Backend de aplicação	g.adbet77.com → AWS ELB sa-east-1 (São Paulo) · 18.231.90.133 (AS16509 Amazon)
Indício de build	caminho Jenkins no código: gameset-v8-h5-to-prod-**k2** · IP interno 15.229.111.138 (AWS São Paulo)
Servidor web	Server: cloudflare (origem não exposta) · porta 80 → 301 HTTPS
Certificado TLS	CN=7play77.com · emissor Let's Encrypt E7 (DV) · válido 06/05/2026–04/08/2026
Série / Fingerprint	0555326151716F2A…4337FD2 · SHA-256 45:13:30:CF:6A:30:0C:F6:B8:33:5C:12:79:1C:2C:54…
Histórico (crt.sh)	3 emissões desde 06/05/2026 (dia do registro): Let's Encrypt, Google Trust, Amazon

Leitura técnica. Registro recente, validade de 1 ano e titular oculto compõem um perfil de **baixa rastreabilidade do responsável**. O uso de **Cloudflare como proxy oculta o IP de origem**, dificultando a localização do servidor que efetivamente armazena dados e processa pagamentos; mesmo assim, a configuração da aplicação expõe o backend em `g.adbet77.com` sobre AWS São Paulo. 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 (Gandi), à Cloudflare nem à Amazon (AWS), meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site entrega um **cassino online de "slots" e apostas** em português (pt-BR), construído como SPA (Vue / build "h5-v8-k2"). A lógica de negócio é servida por uma **API em domínio próprio separado** (`g.adbet77.com`), com área de cadastro/login, carteira, depósito/recarga, saque, bônus de primeiro/segundo depósito, "cashback" de perdas e um **programa de afiliados/indicação** multinível (rotas `/agent/v1/…` e `/activity/inviteChest/…`). O depósito e o saque são feitos por **PIX** (endpoints `/pay/v1/payInOrder` e `/pay/v1/payOutOrder`). O motor de jogos é externo (`game.getpggame.com` · WebSocket `gateway.game-api7.com`).

Aspecto	Constatação
Tipo de serviço	Cassino online de slots e apostas (plataforma "7PLAY77")
Tecnologia	SPA Vue atrás de Cloudflare · API em g.adbet77.com (AWS São Paulo) · build white-label "gameset-v8-h5-k2"
Meio de pagamento	Depósito e saque via PIX (/pay/v1/payInOrder · payOutOrder)
Intermediário (gateway)	Não nomeado no front-end — PIX intermediado pelo próprio backend do operador (g.adbet77.com)
Dados pessoais coletados	CPF, nome, e-mail, telefone, senha e dados bancários (banco/conta) para saque
Identificação do operador	**Ausente** — sem CNPJ real, razão social ou endereço; só o placeholder de template 00.000.000/0000-00
Autorização / licença	**Ausente** — sem selo SPA/SIGAP; apenas alegação genérica de "licença de jogos dos EUA" (não verificável)
Domínio	.com (genérico) — **não** o padrão .bet.br exigido das casas autorizadas no Brasil
Contato divulgado	Suporte via Telegram (t.me) · sem canal corporativo identificável
Aviso de idade	Checkbox "Tenho +18 anos" nos Termos de Uso (genérico)

Leitura técnica. O fluxo financeiro é real e operante: o usuário deposita por PIX e fornece CPF, senha e dados bancários. O **risco não está na tecnologia, mas na ausência de responsável identificável e de autorização**: não há a quem cobrar prêmios/saques não pagos, nem garantia de tratamento adequado dos dados. A arquitetura (front white-label "k2" no domínio público + API em outro domínio + Cloudflare ocultando a origem) é típica de **plataformas de cassino replicadas em escala**, em que vários sites compartilham o mesmo backend. 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 PIX.
Imagens. Os assets gráficos baixados (logo "777.png", favicon, ícones de menu) são PNGs web otimizados, **sem metadados EXIF/GPS/autor** (campos removidos) — coerente com material de template. A imagem social declarada no HTML (og:image 856×480 JPEG) **não corresponde** ao arquivo real entregue (480×161 PNG), indício de metatags de modelo não ajustadas. Ver `imagens/metadata_exiftool.txt`.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Cassino/apostas sem identificação do operador (CNPJ real/razão social/endereço)	`corpo_https.html · app_main_js.js`	ALTA
2	Sem indício de autorização federal (SPA/SIGAP); em .com, não .bet.br	`app_main_js.js · RDAP`	ALTA
3	Recebe PIX e coleta CPF/senha/dados bancários sem responsável localizável	`app_main_js.js · app_env_js.js`	ALTA
4	Origem mascarada por Cloudflare (IP do servidor real oculto)	`dns_records.txt · headers_https.txt`	MÉDIA
5	Domínio recém-registrado (~5 semanas), validade de 1 ano	`RDAP — 06/05/2026`	MÉDIA

6	Titular oculto (privacidade de registro)	`RDAP — só registrador`	MÉDIA
7	Programa de afiliados/indicação multinível com comissão	`app_main_js.js`	MÉDIA
8	Plataforma white-label replicável (build "k2"; API em g.adbet77.com)	`app_env_js.js`	MÉDIA
9	Alegação genérica e não verificável de "licença de jogos dos EUA"	`app_main_js.js`	BAIXA
10	Suporte só por Telegram; sem e-mail próprio (sem MX/TXT)	`app_main_js.js · dns_records.txt`	BAIXA

Síntese: 3 indicadores de severidade ALTA, 5 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (operador identificado, autorização brasileira, contato corporativo, histórico) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 10/06/2026, conclui-se que **7play77.com** é um **cassino online de slots/apostas em operação**, voltado ao público brasileiro (pt-BR, BRL, CPF, PIX), que recebe depósitos via PIX e coleta dados pessoais e bancários, porém **sem identificar quem o opera** e **sem qualquer indício de autorização** para explorar jogos de azar/apostas no Brasil — usando domínio **.com** em vez do padrão regulado **.bet.br**, com a origem mascarada por Cloudflare e a lógica em um backend white-label compartilhável (g.adbet77.com). Soma-se a isso o registro recente, o titular oculto e o contato limitado a um canal de Telegram. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não se cadastrar, não depositar e não fornecer CPF, senha, dados bancários ou pessoais** ao site.
- Desconfiar de anúncios e mensagens (Instagram, WhatsApp, Telegram, SMS) que conduzam a `7play77.com` 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 cassino/apostas sem autorização, e reportar aos canais de abuse do registrador (Gandi), da Cloudflare e da Amazon (AWS), 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.

— Fim do relatório —

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