RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

3887win.com

Objeto investigado	3887win.com — cassino/apostas online (slots) (gTLD .com)
Natureza	Verificação de legitimidade, de risco ao consumidor e do recebedor PIX
Data da coleta	24/06/2026 (RDAP, DNS, HTTP/TLS, geolocalização, app, PIX)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do app · decodificação BR Code (PIX)
Achado central	Cassino sem identificação do operador e sem autorização; PIX a terceiro (WALRUS LTDA)
Classificação	**RISCO ALTO**
Emissão do laudo	24/06/2026 às 03:21

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **3887win.com**, realizada em **24/06/2026** 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 (cadeia de custódia).

O domínio **está no ar** e entrega um **cassino online de "slots" / apostas em português**, construído como aplicação de página única (SPA, build Vite) servida atrás da **Cloudflare**. O aplicativo oferece **cadastro, carteira, depósito e saque via PIX**, **bônus** e **programa de indicação**, e integra catálogos de jogos de provedores de terceiros (Pragmatic Play, JDB, CQ9, Spribe, JILI, TADA). O cadastro coleta **CPF, nome, e-mail, telefone e senha**. A página carrega ainda um **pixel de rastreamento publicitário** (`api.imotech.video`), compatível com tráfego pago para captação de apostadores.

O conjunto de sinais é o de uma operação **opaca e sem lastro verificável**: domínio **recém-registrado** (17/05/2026), **titular oculto**, infraestrutura de origem **mascarada por Cloudflare**, e — no próprio site — **nenhuma identificação do operador** (sem CNPJ, razão social ou endereço), **nenhum selo de autorização regulatória brasileira** e metadados de página em branco (título e Open Graph vazios, típicos de template não preenchido). A marca pública "3887win" **não corresponde** ao recebedor do PIX.

A decodificação do **código PIX "copia e cola"** (BR Code/EMV) fornecido confirma que o pagamento é liquidado em favor de **WALRUS LTDA** (São Paulo), por meio do provedor de pagamento **Hyper Wallet** (`qrcode.hyperwalletip.com.br`) — ou seja, **o dinheiro vai para um terceiro cujo nome não é o da marca anunciada**. No Brasil, a exploração de apostas/jogos de azar online 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, sem qualquer indício de autorização — perfil compatível com **operação irregular/não autorizada**, sujeita a bloqueio pelas autoridades brasileiras.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: uma plataforma que recebe dinheiro (PIX) e dados sensíveis (CPF, senha) **sem identificar quem a opera nem comprovar autorização**, e cujo recebedor de pagamento é um terceiro distinto da marca, 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 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 (arquivo `hash_manifest.txt`). O DNS foi consultado via resolvedor público 1.1.1.1. O conteúdo HTTPS, os cabeçalhos e o aplicativo JavaScript foram coletados por requisição equivalente à de um visitante comum (curl/openssl). O código PIX "copia e cola" foi decodificado segundo o padrão EMV/BR Code (TLV), com verificação do CRC16. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Verisign / .com — registrador Name SRS AB)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS e porta 80	`corpo.html` · `headers_https.txt` · `headers_http80.txt`
Aplicação (front-end)	Download do bundle JS do site	`index.js`

Certificado TLS	openssl s_client / x509	`tls_info.txt`
Geolocalização do IP	ipinfo.io · ip-api.com	`geo_ipinfo_*.json · geo_ipapi_*.json`
Recebedor PIX	Decodificação BR Code (EMV/TLV) + CRC16	`pix_decode.txt`
Provedor de pagamento	RDAP (.br) + CNPJ público (cnpj.ws)	`rdap_hyperwalletip.json · cnpj_interm.json`

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

Domínio	3887win.com (gTLD .com — Verisign)
Registro	**17/05/2026** · expira 17/05/2027 (validade de 1 ano) · alt. 19/05/2026
Idade na coleta	**~5 semanas** — domínio recente
Titular	**Oculto** (privacidade; RDAP expõe só o registrador)
Registrador	Name SRS AB
Status	clientTransferProhibited · DNSSEC não assinado
Servidores de nome	liberty / mack.ns.cloudflare.com (Cloudflare)
DNS — A	172.67.131.23 · 104.21.3.185 (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 (PoPs em San Francisco/Toronto; não revela o servidor real)
Servidor web	Server: cloudflare (origem não exposta) · porta 80 → 301 HTTPS
Conteúdo	last-modified 17/06/2026 · SPA Vite · título e Open Graph vazios (template)
Certificado TLS	CN=3887win.com · emissor Let's Encrypt E7 (DV) · válido 19/05/2026–17/08/2026
Série / Fingerprint	056002D06BB653C75EAFC62D7DE93AD3266A · SHA-256 2E:06:99:53:04:0E:3D:AB:E3:04:A6:FF:FF:FE:D4:28…

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; a geolocalização dos IPs é anycast (PoPs da Cloudflare) e **não indica a localização real** da operação. 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 (Name SRS) nem à Cloudflare, 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 (build Vite). O aplicativo possui área de cadastro/login, carteira, depósito/recarga, saque, **bônus** e um **programa de afiliados/indicação**, e agrega catálogos de jogos de **provedores de terceiros** (Pragmatic Play, JDB, CQ9, Spribe, JILI, TADA). O depósito e o saque são feitos por **PIX**. O código referencia ainda uma marca irmã (`444tiger.win`) e carrega um pixel de rastreamento publicitário (`api.imotech.video`).

Aspecto	Constatação
Tipo de serviço	Cassino online de slots e apostas (marca "3887win")
Tecnologia	SPA Vite atrás de Cloudflare · agregador de jogos de terceiros · pixel api.imotech.video
Meio de pagamento	Depósito e saque via PIX (QR dinâmico "copia e cola")
Provedor de pagamento (PSP)	Hyper Wallet — qrcode.hyperwalletip.com.br (Hyper Wallet Inst. de Pagamento Ltda, CNPJ 07.136.847/0001-47, SP, ativa)
Recebedor do PIX	**WALRUS LTDA** (São Paulo) — **não corresponde** à marca anunciada "3887win"
Dados do BR Code	Moeda BRL (986) · QR dinâmico (valor/txid no ato) · CRC16 A1F7 verificado e íntegro
Dados pessoais coletados	CPF, nome, e-mail, telefone e senha (cadastro e saque)
Identificação do operador	**Ausente** — sem CNPJ, razão social ou endereço da casa no site
Autorização / licença	**Ausente** — sem selo SPA/SIGAP; sem "jogo responsável"
Domínio	.com (genérico) — **não** o padrão .bet.br exigido das casas autorizadas no Brasil
Aviso de idade	Menção genérica "18+" no conteúdo

Leitura técnica. O fluxo financeiro é real e operante: o usuário deposita por PIX e fornece CPF e senha. O **risco não está na tecnologia, mas na ausência de responsável identificável e de autorização**, agravada por um achado relevante: **o recebedor do PIX (WALRUS LTDA) não é a marca anunciada**. O pagamento é intermediado pela Hyper Wallet, instituição de pagamento regularmente inscrita (CNPJ ativo) — o que **não atesta a legitimidade do estabelecimento** que usa o serviço, apenas que o trânsito do dinheiro passa por um PSP cadastrado. Não se imputa conduta ilícita à Hyper Wallet, provedora de pagamento; a divergência entre marca e recebedor, somada à opacidade do operador, é que sustenta a classificação de risco.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Cassino/apostas sem identificação do operador (CNPJ/razão social/endereço)	`corpo.html · index.js`	ALTA
2	Sem indício de autorização federal (SPA/SIGAP); em .com, não .bet.br	`index.js · RDAP`	ALTA
3	Recebedor do PIX (WALRUS LTDA) diverge da marca anunciada "3887win"	`pix_decode.txt`	ALTA
4	Recebe PIX e coleta CPF/senha sem responsável localizável	`index.js · pix_decode.txt`	ALTA
5	Origem mascarada por Cloudflare (IP do servidor real oculto)	`dns_records.txt · headers_https.txt`	MÉDIA
6	Domínio recém-registrado (~5 semanas), validade de 1 ano	`RDAP — 17/05/2026`	MÉDIA
7	Titular oculto (privacidade de registro)	`RDAP — só registrador`	MÉDIA
8	Metadados de página vazios (título/Open Graph em branco — template)	`corpo.html`	MÉDIA

9	Pixel de rastreamento publicitário (tráfego pago para captação)	`corpo.html · index.js`	BAIXA
10	Marca irmã referenciada (444tiger.win) — padrão replicável	`index.js`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 4 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (operador identificado, autorização brasileira, recebedor coincidente com a marca, contato corporativo) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 24/06/2026, conclui-se que **3887win.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, 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. A decodificação do PIX demonstra que os pagamentos são liquidados em favor de **WALRUS LTDA**, terceiro cujo nome **não coincide** com a marca anunciada, via o PSP Hyper Wallet. Somam-se a isso o registro recente, o titular oculto e a página com metadados de template em branco. 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 `3887win.com` ou prometam bônus/ganhos fáceis.
- Se já houve depósito: acionar o banco e o mecanismo **MED** do PIX, reunir comprovantes (inclusive o recebedor **WALRUS LTDA**) 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 (Name SRS) e da Cloudflare, anexando este laudo.
- Comunicar ao PSP **Hyper Wallet** e ao Banco Central a divergência entre a marca anunciada e o recebedor (**WALRUS LTDA**), para verificação de uso indevido do arranjo de pagamento.
- Preservar este relatório e as evidências (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 (Cloudflare, Name SRS, Hyper Wallet).

— Fim do relatório —

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