RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do endereço

moleca-store.vercel.app

Objeto investigado	moleca-store.vercel.app — loja de calçados que se apresenta como "Moleca" (subdomínio gratuito Vercel)
Natureza	Verificação de legitimidade e de risco ao consumidor (apropriação de marca)
Data da coleta	08/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise do app e do PIX)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do app · decodificação do BR Code (PIX)
Achado central	Loja SEM domínio e SEM CNPJ próprios, que usa a marca "Moleca"; PIX vai a intermediário, não à loja
Classificação	**RISCO ALTO**
Emissão do laudo	08/07/2026 às 16:17

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **moleca-store.vercel.app**, realizada em **08/07/2026** 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.

O endereço **não é um domínio próprio**: é um **subdomínio gratuito** (`moleca-store`) criado sob o domínio `vercel.app`, da plataforma de publicação **Vercel**. Ou seja, **o operador não registrou nenhum domínio** — apenas publicou um site na infraestrutura gratuita da Vercel, o que **elimina o registro de domínio como fonte de identificação** do responsável (o titular da conta Vercel não é público). A página é uma aplicação de página única (SPA React/Vite) intitulada **"Páscoa Moleca — Promoção Especial"** que reproduz a identidade visual da marca de calçados **Moleca** (marca da Calçados Beira Rio S.A.), inclusive **reutilizando fotos de produto hospedadas em uma loja Shopify de terceiros** e exibindo **selos falsos** ("Google", "Norton", "Reclame Aqui").

O site coleta **nome, e-mail, telefone/WhatsApp, CEP, endereço, cidade, estado e CPF** e conduz o comprador a um **pagamento por PIX** gerado por uma função de servidor da própria Vercel (`/api/pix`), a qual aciona um **intermediário de pagamento** (`qrcode.fyhub.com.br`). A decodificação do código PIX "copia e cola" fornecido confirma que o **recebedor não é a loja "Moleca"**, mas um beneficiário genérico identificado como **"SISTEMA DE INTERMEDIACAO"** (São Paulo) — isto é, **o dinheiro não vai para um CNPJ da loja anunciada**, e sim para um agregador de pagamentos, o que oculta o beneficiário final. Há ainda captura de "leads" (`/api/capture`: nome, e-mail e telefone enviados ao operador) e um **TikTok Pixel**, compatível com captação de vítimas por **tráfego pago**.

O conjunto de sinais — ausência de domínio e de CNPJ próprios, uso não autorizado de marca de terceiro, preços irrisórios, selos de confiança forjados, contato limitado a um Gmail e a um WhatsApp, e pagamento a um intermediário em vez de à loja — é **típico de loja falsa / golpe de e-commerce**. Classifica-se o caso como **RISCO ALTO** ao consumidor.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: quando um site **não tem domínio nem CNPJ próprios**, exibe marca de terceiro sem autorização e envia o pagamento a um **intermediário** (e não à loja anunciada), o consumidor fica sem qualquer responsável localizável para cobrar entrega ou reembolso. Recomenda-se **não comprar, não pagar o PIX 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. Como o alvo é um **subdomínio de plataforma de deploy** (Vercel), o registro (RDAP) foi consultado sobre o domínio-base `vercel.app` — que identifica a **plataforma**, não o operador do site. O DNS foi consultado via resolvedor público 8.8.8.8; o conteúdo e os cabeçalhos, por requisição HTTP de visitante comum. O código PIX "copia e cola" informado pelo solicitante foi preservado e decodificado pelo padrão EMV/BR Code (TLV). Fuso de referência: horário de Brasília.

Etapa	Técnica / fonte	Evidência preservada
Registro (plataforma)	RDAP do domínio-base vercel.app (Google Registry / Tucows)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, SOA, MX, TXT, CNAME)	`dns_records.txt`
Conteúdo / cabeçalhos	curl (HTTPS e porta 80) — visitante comum	`corpo.html` · `headers_https.txt` · `headers_http80.txt`

Aplicação (front-end)	Download do bundle JS do site (Vite)	`app_index-BBjH8NhC.js`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ip-api.com	`geo_ip.txt`
Intermediário PIX	RDAP (registro.br) + DNS de fyhub.com.br	`rdap_fyhub.json`
Código PIX	Decodificação EMV/BR Code (TLV) do copia e cola	`pix_copiaecola.txt`

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

Endereço	moleca-store.vercel.app — **subdomínio gratuito**, não um domínio próprio
Domínio próprio	**Inexistente** — o operador não registrou domínio; publicou site na Vercel
Plataforma de deploy	**Vercel Inc.** (plataforma de publicação gratuita/self-service)
Registro do domínio-base	vercel.app registrado pela Vercel em 28/01/2020 (Google Registry / registrador Tucows) — **não identifica o operador do site**
Titular do site	**Não público** — apenas o dono da conta Vercel, não exposto em base de registro
DNS — A	216.198.79.2 · 64.29.17.2 (rede Vercel/AWS) · sem MX · sem TXT/SPF
Servidores de nome	ns1–ns4.vercel-dns-3.com (Vercel)
Hospedagem	Vercel, Inc. sobre AWS (AS16509 Amazon) · borda em GRU (São Paulo) · Server: Vercel
Geolocalização do IP	Rede de borda da Vercel/AWS (não revela o operador nem um endereço físico próprio)
Certificado TLS	curinga `*.vercel.app` — emissor Google Trust Services (WR1, DV) · válido 28/06/2026–26/09/2026
Identidade no certificado	**Nenhuma** — certificado é da plataforma Vercel, não do operador nem da marca "Moleca"
Porta 80	redireciona (308) para HTTPS
Última publicação	build servido com last-modified de 08/07/2026 (redeploy recente)

Leitura técnica. Este é o cenário — cada vez mais comum — de **site sem domínio próprio**: o golpista não registra domínio (o que deixaria rastro em RDAP/WHOIS) e apenas **hospeda um clone em plataforma de deploy gratuita** (aqui, a Vercel). Em consequência, o RDAP do `vercel.app` devolve apenas os dados da **plataforma**, e o certificado TLS curinga `*.vercel.app` é da **própria Vercel** — nenhum deles identifica quem opera o site ou comprova vínculo com a marca "Moleca". Não se imputa qualquer conduta à Vercel nem à Amazon (AWS), meros provedores de infraestrutura; o subdomínio, porém, é um forte candidato a **denúncia de abuso** junto à plataforma para retirada do ar (Seção 6).

4. Conteúdo, Fluxo de Pagamento (PIX) e Dados Coletados

A página entrega uma **loja de calçados** em português que se apresenta como a marca **Moleca** ("Páscoa Moleca — Promoção Especial"), com preços irrisórios. As fotos de produto e banners são **carregados diretamente de uma loja Shopify de terceiros** (`cdn.shopify.com` · conta `diadamulheermuleca.myshopify.com`), e a página exibe **selos de confiança forjados** ("Google", "Norton", "Reclame Aqui") — imagens estáticas, sem qualquer verificação real. O pagamento é feito por **PIX**, gerado no servidor pela função `/api/pix` da Vercel, que aciona o intermediário `qrcode.fyhub.com.br`; o status é consultado por `/api/check-pix`. Há ainda `/api/capture`, que envia **nome, e-mail e telefone** do visitante ao operador ("capturar lead"), e um **TikTok Pixel** de rastreamento de anúncios.

Decodificação do código PIX (EMV / BR Code) informado

Campo	Conteúdo	Interpretação
`00`	01	Payload Format Indicator
`26`	GUI br.gov.bcb.pix · URL qrcode.fyhub.com.br/qr/v3/at/5f52017b-8154-4d5b-85a1-f6505924ef4f	PIX dinâmico via **intermediário fyhub** (payload hospedado por terceiro)
`52`	0000	MCC não informado
`53`	986	Moeda: BRL (Real)
`58`	BR	País: Brasil
`59`	SISTEMA_DE_INTERMEDIACAO_	**Recebedor genérico — NÃO é a loja "Moleca"** (agregador de pagamentos)
`60`	SAO_PAULO	Cidade do recebedor
`62`	txid = ***	Identificador da transação mascarado
`63`	48DA	CRC16 de verificação

Aspecto	Constatação
Tipo de serviço	Loja (e-commerce) de calçados que se apresenta como a marca "Moleca"
Domínio / CNPJ próprios	**Ausentes** — subdomínio gratuito vercel.app; nenhum CNPJ/razão social/endereço da loja
Uso de marca	Marca "Moleca" (Calçados Beira Rio S.A.) usada sem indício de autorização; fotos de produto de loja Shopify de terceiros
Meio de pagamento	PIX dinâmico gerado no servidor (/api/pix) via intermediário qrcode.fyhub.com.br
Recebedor do PIX	**"SISTEMA DE INTERMEDIACAO" (São Paulo)** — agregador, não a loja anunciada
Intermediário (fyhub)	fyhub.com.br — registro.br 29/08/2025; titular Matheus Veloso Horst; backend qrcode.fyhub.com.br → fyhub-prod.onz.software (AWS São Paulo)
Dados pessoais coletados	Nome, e-mail, telefone/WhatsApp, CEP, endereço (via ViaCEP), cidade, estado e CPF
Captura de leads	/api/capture envia nome, e-mail e telefone ao operador (notificação em segundo plano)
Selos de confiança	**Forjados** — imagens "Google", "Norton" e "Reclame Aqui" sem verificação real
Rastreamento / anúncios	TikTok Pixel (sdkid D7K4V9JC77U1C1VBG7GG) — compatível com captação por tráfego pago
Contato divulgado	E-mail moleca@gmail.com (Gmail gratuito) · WhatsApp +55 21 95943-3111 — sem canal corporativo

Leitura técnica. O ponto central do golpe está na cadeia de pagamento: o comprador acredita pagar à loja "Moleca", mas o BR Code aponta a um **recebedor genérico de intermediação**, sem CNPJ da loja — padrão que **oculta o beneficiário final** e dificulta

o ressarcimento. Não se imputa conduta ilícita ao intermediário de pagamento (fyhub) nem ao provedor de infraestrutura PIX (Onz): são citados como fato técnico; o uso concreto da conta é que deve ser apurado pelos canais competentes. A combinação de site sem domínio/CNPJ próprios, marca de terceiro, selos forjados e preços irrisórios caracteriza **loja falsa**.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Recebedor do PIX é "intermediação" genérica, não a loja anunciada (sem CNPJ da loja)	`pix_copiaecola.txt`	ALTA
2	Uso da marca "Moleca" e de fotos de terceiros (Shopify) sem indício de autorização	`corpo.html · app_index-BBjH8NhC.js`	ALTA
3	Sem domínio e sem identificação (CNPJ/razão social/endereço) do operador	`RDAP vercel.app · app JS`	ALTA
4	Selos de confiança forjados ("Google", "Norton", "Reclame Aqui")	`app_index-BBjH8NhC.js`	ALTA
5	Coleta CPF, endereço e contato e captura leads (/api/capture) para o operador	`app_index-BBjH8NhC.js`	MÉDIA
6	Site hospedado em subdomínio gratuito de plataforma de deploy (Vercel)	`headers_https.txt · DNS`	MÉDIA
7	Preços irrisórios / promoção de forte apelo ("Páscoa Moleca")	`corpo.html · app JS`	MÉDIA
8	TikTok Pixel — captação de vítimas por tráfego pago	`corpo.html`	MÉDIA
9	Contato apenas por Gmail gratuito e WhatsApp; sem canal corporativo	`app_index-BBjH8NhC.js`	BAIXA
10	Intermediário PIX (fyhub) recém-registrado (ago/2025), titular pessoa física	`rdap_fyhub.json`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 4 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (loja/operador identificado, domínio e CNPJ próprios, autorização de uso da marca, contato corporativo) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 08/07/2026, conclui-se que **moleca-store.vercel.app** é uma **loja falsa** que se apropria da identidade da marca de calçados **Moleca**, publicada em um **subdomínio gratuito da plataforma Vercel — sem domínio próprio, sem CNPJ, sem razão social e sem endereço** que identifiquem um responsável. O comprador é induzido a fornecer dados pessoais (inclusive CPF) e a pagar por **PIX** cujo recebedor, conforme decodificação do BR Code, é um **agregador de pagamentos genérico ("SISTEMA DE INTERMEDIACAO")**, e não a loja anunciada. Somam-se selos de confiança forjados, fotos de terceiros, preços irrisórios e captação por tráfego pago (TikTok Pixel). Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não comprar, não pagar o PIX e não fornecer CPF, endereço ou dados pessoais** ao site.
- Desconfiar de anúncios e mensagens (Instagram, TikTok, WhatsApp) que ofereçam calçados "Moleca" com desconto agressivo e conduzam a `moleca-store.vercel.app`. Comprar apenas em canais oficiais da marca (Calçados Beira Rio) ou em lojas com CNPJ verificável.
- Se já houve pagamento: acionar o banco e o mecanismo **MED** do PIX o quanto antes, reunir comprovantes e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência.

Recomendações de mitigação / denúncia

- Denunciar o subdomínio ao **canal de abuso da Vercel** (o site viola termos de uso ao usar marca de terceiro em plataforma gratuita) para **retirada do ar**, anexando este laudo.
- Comunicar a **Calçados Beira Rio S.A.** (detentora da marca Moleca) sobre o uso indevido da marca, e reportar o recebedor PIX ao **intermediário (fyhub / Onz)** e ao banco do recebedor para bloqueio da conta usada no golpe.
- Preservar este relatório e as evidências (com hashes SHA-256) para eventual uso administrativo ou judicial.

Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do endereço 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 (Vercel, AWS) e de pagamento (fyhub, Onz) citados, meros intermediários; o uso concreto das contas deve ser apurado pelos canais competentes.

— Fim do relatório —

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