RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

superspetz.com

Objeto investigado	superspetz.com — loja on-line de produtos para pets (gTLD .com)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	19/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise do app, PIX)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo/app · decodificação de BR Code PIX
Achado central	Pagamento só por PIX cujo recebedor é PESSOA FÍSICA (YANA CLARA), divergente da loja/CNPJ anunciados
Classificação	**RISCO ALTO**
Emissão do laudo	19/07/2026 às 09:59

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **superspetz.com**, realizada em **19/07/2026** 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 domínio **está no ar** e entrega uma **loja on-line de produtos para animais de estimação** em português (título "Superspetz — A super loja para o seu pet"), construída como aplicação de página única servida atrás da **Cloudflare** sobre a plataforma de criação de sites **Lovable** (host `l5e.io`), com backend **Supabase**. O checkout coleta **nome, e-mail, telefone, CPF e endereço** e oferece pagamento **exclusivamente por PIX**, com o código "copia e cola" (BR Code EMV) **gerado no próprio navegador**, **sem intermediário/gateway de pagamento**.

A análise do código PIX fornecido pelo solicitante é o achado central. O BR Code é válido (CRC16 confere) e paga para uma **chave PIX aleatória** cujo recebedor é **YANA CLARA** — **pessoa física**, na cidade de São Paulo, no valor de **R$ 72,23**. Esse recebedor **não corresponde** à loja anunciada. O site se apresenta como **SUPER PETZ LTDA**, CNPJ `58.669.083/0001-96` (Porto Alegre/RS); a consulta à base pública da Receita confirma que esse CNPJ **existe e está ativo**, mas seu único sócio-administrador é **Henry Bastos dos Santos** — ou seja, o dinheiro **não vai para a conta da pessoa jurídica anunciada nem para o seu sócio**, e sim para a chave pessoal de um terceiro. Pagamento direto a pessoa física, sem gateway e com recebedor divergente do estabelecimento, **retira do consumidor as proteções** associadas a uma conta lojista.

Somam-se sinais convergentes: **domínio recém-registrado** (05/06/2026), **titular oculto**, nome "Super Petz"/"superspetz" **semelhante à marca notória de terceiro** ("Petz"), **fotos de produto hospedadas em lojas alheias** (hotlink de `nutrimais.com` e `images.tcdn.com.br`), **preço menor exclusivo para PIX** e **pixels de anúncio** (Google Ads e Meta) compatíveis com captação por tráfego pago. O conjunto configura **RISCO ALTO** ao consumidor.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: uma loja que só aceita PIX para uma **chave pessoal de terceiro**, sem gateway e com recebedor que não é o estabelecimento anunciado, expõe o consumidor ao risco de **pagar e não receber**, sem canal de estorno lojista. Recomenda-se **não pagar por esse PIX e não fornecer dados pessoais** (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 código PIX "copia e cola" foi fornecido como texto pelo solicitante, preservado em arquivo e decodificado pelo 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 NameCheap)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME, PTR)	`dns_dig.txt`
Conteúdo / cabeçalhos	curl HTTPS (corpo + cabeçalhos)	`corpo_https.html` · `http_headers_https.txt`
Aplicação (front-end)	Download dos bundles JS (checkout, PIX, admin, sobre)	`js_*.js`

Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · ip-api.com · PTR reverso	`ip_geolocalizacao.json`
Identidade PJ alegada	Consulta pública de CNPJ (Receita via BrasilAPI)	`cnpj_58669083000196.json`
Código PIX	Decodificação EMV/BR Code (TLV) + CRC16	`pix_copiaecola.txt`
Imagens	Download de assets · exiftool	`imagens/ · metadata_exiftool.txt`

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

Domínio	superspetz.com (gTLD .com — Verisign)
Registro	**05/06/2026** · expira 05/06/2027 (validade de 1 ano) · última alteração 02/07/2026
Idade na coleta	**~6 semanas** — domínio recente
Titular	**Oculto** (privacidade; RDAP expõe só o registrador)
Registrador	NameCheap, Inc.
Status	active
Servidores de nome	ganz / luciane.ns.cloudflare.com (Cloudflare)
DNS — A	185.158.133.1 (apex e www) · sem AAAA
MX / TXT	eforward1-5.registrar-servers.com (encaminhamento NameCheap) · SPF de encaminhamento
PTR reverso	185.158.133.1 → `lovable-app-cd-1-4.p.l5e.io` (plataforma Lovable)
Hospedagem (borda)	AS13335 Cloudflare, Inc. — proxy/CDN sobre a plataforma Lovable (l5e.io)
Geolocalização do IP	Anycast Cloudflare (não revela a localização do servidor real)
Backend de aplicação	Supabase — `cakoqdolvlypofuhaawt.supabase.co` (BaaS)
Cabeçalhos reveladores	Server: cloudflare · x-deployment-id presente · cf-ray …-GRU (borda São Paulo)
Certificado TLS	CN=superspetz.com · emissor Google Trust Services WE1 (DV) · válido 16/06/2026–14/09/2026
Série / Fingerprint	CF49C7AC889425A413BAD234CCA255F2 · SHA-256 49:D5:90:C9:81:08:63:BF:83:C0:1A:C0:0D:E9:37:EE…

Leitura técnica. Registro recente, validade de 1 ano e titular oculto compõem um perfil de **baixa rastreabilidade do responsável**. O site não tem infraestrutura própria: é publicado na plataforma de criação **Lovable** (PTR `l5e.io`) com backend **Supabase**, atrás da **Cloudflare**, que oculta o IP de origem. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. Não se imputa conduta ao registrador (NameCheap), à Cloudflare, à Lovable nem ao Supabase — meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é uma **loja on-line de produtos para pets** (rações, antipulgas, brinquedos, acessórios) em pt-BR, com catálogo por categorias (cães, gatos, pássaros, peixes, pequenos, farmácia). O pagamento é **exclusivamente por PIX**: o código "copia e cola" (BR Code EMV) é **montado no próprio navegador** a partir de configurações do operador (chave, nome e cidade do recebedor definidos em um painel administrativo interno `/admin/pix`), **sem qualquer gateway de pagamento**. O checkout coleta dados pessoais e de entrega. As fotos de produto do catálogo são **carregadas diretamente de servidores de outras lojas** (`nutrimais.com`, `images.tcdn.com.br`).

Decodificação do código PIX (EMV/BR Code)

Recebedor (campo 59)	**YANA CLARA** — pessoa física
Cidade (campo 60)	SAO PAULO
Chave PIX (campo 26)	**Aleatória** — 1d5f73e7-2907-483e-9004-d9a27598f814 (GUI br.gov.bcb.pix)
Valor (campo 54)	R$ 72,23 · moeda 986 (BRL) · país BR
Tipo (campo 01)	11 — QR reutilizável
txid (campo 62)	SP59593156D8Y
CRC16 (campo 63)	3ADB — **válido** (confere com o payload)
Intermediário / gateway	**Nenhum** — PIX direto para chave pessoal, sem agregador

Identidade jurídica anunciada vs. recebedor

Loja anunciada (página "Sobre")	SUPER PETZ LTDA · CNPJ 58.669.083/0001-96 · Rua Senhor do Bom Fim, 1033, Sarandi, Porto Alegre/RS
CNPJ na base pública	**Existe e está ATIVO** — SUPER PETZ LTDA, aberto em 07/01/2025, comércio varejista de artigos/alimentos para pets, mesmo endereço
Sócio-administrador (CNPJ)	Henry Bastos dos Santos
Recebedor do PIX	**YANA CLARA** (pessoa física) — **não é a empresa nem o sócio**

Leitura técnica. Ainda que o CNPJ exibido seja real e ativo, o **dinheiro não é recebido pela pessoa jurídica anunciada**: o PIX aponta para a **chave pessoal de um terceiro** (Yana Clara), que não consta como sócia da SUPER PETZ LTDA. A geração do BR Code no próprio navegador, **sem gateway**, e o recebedor divergente do estabelecimento significam que **não há conta lojista com mecanismos de estorno/contestação** por trás do pagamento. Somado ao domínio recente, ao nome semelhante à marca notória "Petz" e às fotos de produto hotlinkadas de outras lojas, o padrão é o de **loja montada rapidamente para captar pagamentos por PIX**. Não se afirma, aqui, participação da empresa cujo CNPJ foi exibido; registra-se apenas que o **fluxo financeiro não corresponde a ela**.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Recebedor do PIX é pessoa física (YANA CLARA), divergente da loja/CNPJ anunciados e do sócio da empresa	`pix_copiaecola.txt` · `cnpj_58669083000196.json`	ALTA
2	Pagamento só por PIX, BR Code gerado no navegador, sem gateway/intermediário (sem estorno lojista)	`js_checkout` · `js_index`	ALTA
3	Domínio recém-registrado (~6 semanas), validade de 1 ano, titular oculto	`rdap_raw.json`	ALTA

4	Nome "Super Petz"/"superspetz" semelhante à marca notória de terceiro ("Petz")	`corpo_https.html`	MÉDIA
5	Fotos de produto hotlinkadas de outras lojas (nutrimais.com, images.tcdn.com.br)	`js_index.js`	MÉDIA
6	Coleta CPF, nome, e-mail, telefone e endereço no checkout sem responsável PJ pelo fluxo	`js_checkout.js`	MÉDIA
7	Preço exclusivo menor para pagamento via PIX (incentivo a pagar fora de proteção)	`js_index.js`	MÉDIA
8	Pixels de anúncio (Google Ads AW-18266937258 + Meta Pixel dinâmico) — captação por tráfego pago	`corpo_https.html` · `js_index.js`	MÉDIA
9	Stack no-code descartável (Lovable/l5e + Supabase) atrás de Cloudflare	`tls_cert.txt` · `dns_dig.txt`	BAIXA
10	Contato só por e-mail de encaminhamento (NameCheap); sem canal corporativo verificável	`dns_dig.txt` · `js_index.js`	BAIXA

Síntese: 3 indicadores de severidade ALTA, 5 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (recebedor correspondente à loja, gateway com estorno, marca própria, catálogo próprio) foi constatado no fluxo de pagamento.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 19/07/2026, conclui-se que **superspetz.com** é uma **loja on-line de produtos para pets em operação**, voltada ao público brasileiro, que aceita **somente PIX** para uma **chave pessoal de terceiro** (recebedor **YANA CLARA**, pessoa física), **sem gateway** e com recebedor que **não corresponde** ao estabelecimento anunciado (SUPER PETZ LTDA). Ainda que o CNPJ exibido seja real e ativo, o dinheiro não flui para a pessoa jurídica. O caso reúne domínio recente, titular oculto, nome semelhante à marca notória "Petz", fotos hotlinkadas de outras lojas, incentivo de preço para PIX e pixels de tráfego pago. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não pagar o PIX** e **não fornecer CPF, endereço ou dados pessoais** ao site.
- Desconfiar de anúncios (Instagram, Facebook, Google) que conduzam a `superspetz.com` com ofertas/descontos exclusivos para pagamento via PIX.
- Se já houve pagamento: acionar o banco e o mecanismo **MED** (Mecanismo Especial de Devolução) do PIX, reunir comprovantes e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência.

Recomendações de mitigação / denúncia

- Reportar a **chave PIX aleatória do recebedor** (1d5f73e7-2907-483e-9004-d9a27598f814 · YANA CLARA) ao próprio banco recebedor e ao **Banco Central**, e comunicar o caso à instituição de pagamento para bloqueio/análise.
- Reportar o site aos canais de **abuse** do registrador (NameCheap), da **Cloudflare** e da plataforma **Lovable** (l5e.io), anexando este laudo, para avaliação de remoção.
- Havendo uso indevido de marca semelhante a terceiro ("Petz"), comunicar o **titular da marca** para as providências cabíveis.
- 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, nem à pessoa jurídica cujo CNPJ foi exibido no site.

— Fim do relatório —

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