RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

melissadescontonline.vercel.app

Objeto investigado	melissadescontonline.vercel.app — falsa "Loja Oficial Melissa" de calçados (subdomínio Vercel)
Natureza	Verificação de legitimidade e de risco ao consumidor (e-commerce / marca)
Data da coleta	11/06/2026 (RDAP, DNS, HTTP/TLS, geolocalização, checkout e decodificação PIX)
Métodos	OSINT passivo · RDAP/WHOIS · DNS · HTTP/TLS · análise de conteúdo · BR Code EMV (PIX)
Achado central	Falsa loja Melissa usando CNPJ da Grendene; PIX recebido por "BETRINHA LTDA"
Classificação	**RISCO ALTO**
Emissão do laudo	11/06/2026 às 15:42

1. Sumário Executivo

Este laudo documenta a investigação técnica do site **melissadescontonline.vercel.app**, realizada em **11/06/2026** 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.

O site **está no ar** e se apresenta como **"Melissa — Loja Oficial"**, prometendo calçados da marca Melissa com **"até 97% OFF"**. Trata-se de uma **página estática hospedada na plataforma Vercel** (subdomínio gratuito `*.vercel.app`), montada com **fotos de produtos copiadas de diversas lojas legítimas** (Shopify, VTEX, Tray e outras, carregadas por hotlink) e exibindo no rodapé o **CNPJ 89.850.341/0001-60 — que pertence à Grendene S.A.**, a fabricante real da Melissa. Ou seja, o site **apropria-se da marca e do CNPJ legítimos** do fabricante para passar-se por canal oficial, o que não é.

Ao clicar em "Comprar", o usuário é levado a um **checkout hospedado em domínio distinto e estrangeiro**, `compraonlinesegurada.org.ua` (TLD **.org.ua — Ucrânia**, registrado em 25/02/2026, atrás de Cloudflare), onde são coletados **nome, e-mail, telefone e endereço completo** e é gerado um **pagamento via PIX** intermediado pelo gateway **ParadisePag**. O código PIX "copia e cola" fornecido foi decodificado (padrão EMV/BR Code): o **recebedor é "BETRINHA LTDA" (São Paulo)** — pessoa jurídica que **não corresponde** à "Melissa"/Grendene anunciada —, com a transação roteada pela instituição de pagamento **Treeal** (`pix.treeal.com`).

O conjunto de sinais — uso indevido de marca e CNPJ alheios, descontos irreais (97%), falsa escassez de estoque, fotos de produtos extraídas de terceiros, checkout em domínio estrangeiro recém-criado e PIX para empresa sem relação com a marca — é **típico de loja fraudulenta de e-commerce** ("golpe do PIX"), em que o consumidor paga e não recebe o produto, além de expor seus dados pessoais. Classifica-se o caso como **RISCO ALTO**.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: uma página que se diz "loja oficial" usando marca e CNPJ de terceiros, com preços impossíveis e pagamento por PIX para uma empresa não relacionada, oferece **risco elevado** de prejuízo financeiro e de vazamento de dados. Recomenda-se **não comprar, não pagar o PIX 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 (cadeia de custódia). O DNS foi consultado via `dig`; o conteúdo HTTP/HTTPS via `curl`; o certificado via `openssl`. O código PIX "copia e cola" foi decodificado pelo padrão **EMV/BR Code (TLV)** e o respectivo payload dinâmico (JWS assinado pela instituição de pagamento) foi lido para confirmar o recebedor. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (vercel.app; treeal.com) · WHOIS (.org.ua)	`rdap_vercel_app.json` · `rdap_treeal_com.json` · `whois_checkout.txt`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_dig.txt` · `dns_treeal.txt` · `dns_checkout.txt`
Conteúdo / cabeçalhos	curl (HTTPS e porta 80)	`corpo.html` · `headers_https.txt` · `checkout_corpo.html`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`

Geolocalização do IP	ipinfo.io · ip-api.com · PTR	`geo_ip.txt`
Código PIX (BR Code)	Decodificação EMV/TLV + leitura do JWS dinâmico	`pix_copia_e_cola.txt` · `pix_decodificado.txt` · `treeal_payload_decodificado.txt`
Integridade	sha256sum de todos os artefatos	`hash_manifest.txt`

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

Endereço	melissadescontonline.vercel.app (subdomínio gratuito da plataforma Vercel)
Domínio-base	vercel.app — registrado em 28/01/2020 (plataforma de hospedagem; não é do operador do golpe)
Natureza do endereço	**Subdomínio de aplicação Vercel** — criado por usuário sem registro próprio nem WHOIS individual
Última modificação do conteúdo	28/05/2026 (cabeçalho last-modified) — publicação recente
Servidores de nome	ns1/ns2.vercel-dns.com (Vercel)
DNS — A	64.29.17.194 · 216.198.79.194 (anycast Vercel/AWS) · sem MX · sem TXT/SPF
Hospedagem	Vercel, Inc. sobre AS16509 Amazon AWS — proxy/CDN anycast (Walnut, Califórnia, EUA)
Servidor web	Server: Vercel · x-vercel-cache: HIT
Certificado TLS	CN=*.vercel.app (wildcard da plataforma) · emissor Google Trust Services WR1 (DV)
Validade do TLS	28/04/2026 – 27/07/2026 · série F47D82F2…B294
Fingerprint SHA-256	F8:32:DF:B2:65:37:61:E8:B0:00:1D:BA:F8:4E:AB:20:66:7C:9B:FB:05:20:70:05:47:D3:B3:BF:54:81:43:AA
Checkout (domínio externo)	compraonlinesegurada.org.ua — TLD .org.ua (Ucrânia) · registrado 25/02/2026 · registrador ua.thehost
Checkout — hospedagem	Atrás de Cloudflare (172.67.216.30; NS *.ns.cloudflare.com) — origem oculta
Checkout — contato de registro	e-mail de registrante charlesadebola@gmail.com (base WHOIS .org.ua)

Leitura técnica. O endereço público é um **subdomínio gratuito da Vercel**: não exige registro de domínio nem identifica o responsável, o que favorece a **baixa rastreabilidade** e a remoção/recriação rápida da página. O certificado é um **wildcard da própria plataforma** (*.vercel.app), que comprova apenas o uso da Vercel, **não a identidade de qualquer loja**. O pagamento, porém, ocorre fora da Vercel, em um **checkout sob domínio estrangeiro .org.ua recém-registrado e mascarado por Cloudflare**. Não se imputa conduta à Vercel, à Amazon (AWS) nem à Cloudflare — meros provedores de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é uma **vitrine estática de e-commerce** que se anuncia como **"Melissa — Loja Oficial | Sapatos com até 97% OFF"**. As fotos dos produtos **não são próprias**: são carregadas por hotlink a partir de diversas lojas reais (domínios `cdn.shopify.com`, `*.vtexassets.com`, `images.tcdn.com.br`, `mitiendanube`, entre outros) e de painéis de gateways de pagamento. O logotipo é hospedado em um site Hostinger (`wheat-scorpion-764395.hostingersite.com`). No rodapé, o site exibe o **CNPJ 89.850.341/0001-60**, que é o da **Grendene S.A.** (fabricante legítima da Melissa) — uso indevido para simular oficialidade.

O botão "Comprar" encaminha para o checkout `compraonlinesegurada.org.ua/c/2d01a2cf4d`, que coleta **nome, e-mail, telefone e endereço completo** (CEP via ViaCEP, rua, número, complemento, bairro, cidade, UF), oferece **"order bumps"** (vendas casadas) e gera o **PIX** pelo gateway **ParadisePag** (`paradisepags.com` / `go.paradisepagbr.com`, loja interna "store_3259").

Decodificação do código PIX "copia e cola" (EMV/BR Code)

Campo (EMV)	Conteúdo
26 — Arranjo PIX	GUI br.gov.bcb.pix · URL dinâmica pix.treeal.com/qr/v3/at/d1c30a5e-ca8d-4e45-a1b6-27db5ccf8503
52 — MCC	0000 (categoria não informada)
53 / 58 — Moeda / País	986 (BRL) · BR
59 — Nome do recebedor	**BETRINHA LTDA**
60 — Cidade	SÃO PAULO
63 — CRC16	B993 (válido — código íntegro)
Payload dinâmico (JWS)	Assinado por pix.treeal.com · chave PIX aleatória 737c168c-…-9214df2b0e2e · valor R$ 10,00 · status ATIVA

A URL do arranjo aponta para a **Treeal** (`pix.treeal.com`), instituição de pagamento que processa o PIX via plataforma BaaS (`treeal-prod.onz.software`). O **recebedor de fato é "BETRINHA LTDA"**, de São Paulo — empresa que **não tem relação com a marca Melissa nem com a Grendene** anunciadas no site. Há, portanto, **divergência entre o estabelecimento anunciado e o titular da conta que recebe o dinheiro**.

Aspecto	Constatação
Tipo de serviço	Suposta "loja oficial Melissa" de calçados — vitrine estática (HTML único)
Marca / oficialidade	**Uso indevido** da marca Melissa e do CNPJ da Grendene S.A. (89.850.341/0001-60)
Fotos dos produtos	Hotlink de lojas reais (Shopify, VTEX, Tray etc.) — não são imagens próprias
Checkout / pagamento	Domínio externo .org.ua (Ucrânia) atrás de Cloudflare · PIX via gateway ParadisePag
Recebedor do PIX	**BETRINHA LTDA** (São Paulo) — não corresponde à Melissa/Grendene · via instituição Treeal
Dados pessoais coletados	Nome, e-mail, telefone e endereço completo (CEP, rua, número, bairro, cidade, UF)
Preços	Descontos irreais ("até 97% OFF") — incompatíveis com o varejo legítimo da marca
Gatilhos de urgência	Falsa escassez de estoque e vendas casadas (order bumps) no checkout

Leitura técnica. O conjunto reproduz o padrão clássico de **loja falsa de e-commerce ("golpe do PIX")**: marca e CNPJ de terceiros para simular oficialidade, fotos copiadas, preços impossíveis e pagamento imediato por PIX para uma empresa sem vínculo com a marca. Não se imputa conduta à **Treeal** nem ao gateway **ParadisePag**, instituições de pagamento que apenas processam a cobrança; o ponto relevante é a **incompatibilidade entre o estabelecimento anunciado e o recebedor**, e a impossibilidade de o

consumidor identificar e responsabilizar quem opera o site.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Uso indevido da marca Melissa e do CNPJ da Grendene S.A. (89.850.341/0001-60)	`corpo.html`	ALTA
2	Recebedor do PIX (BETRINHA LTDA) não corresponde ao estabelecimento anunciado	`pix_decodificado.txt` · `treeal_payload_decodificado.txt`	ALTA
3	Checkout em domínio estrangeiro .org.ua recém-registrado (25/02/2026), atrás de Cloudflare	`whois_checkout.txt` · `dns_checkout.txt`	ALTA
4	Descontos irreais ("até 97% OFF") incompatíveis com o varejo legítimo	`corpo.html`	ALTA
5	Fotos de produtos copiadas (hotlink) de diversas lojas reais	`corpo.html`	MÉDIA
6	Página em subdomínio gratuito Vercel, sem responsável identificável	`headers_https.txt` · `rdap_vercel_app.json`	MÉDIA
7	Coleta de dados pessoais e endereço completo em domínio de terceiros	`checkout_corpo.html`	MÉDIA
8	Falsa escassez de estoque e vendas casadas (order bumps) no checkout	`corpo.html` · `checkout_corpo.html`	MÉDIA
9	Logo e assets hospedados em terceiros (Hostinger) e painéis de gateway	`corpo.html`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 4 MÉDIA e 1 BAIXA. **Nenhum fator de legitimidade** (canal oficial verificável, identificação do operador, recebedor coerente com a marca) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 11/06/2026, conclui-se que **melissadescontonline.vercel.app não é** um canal oficial da marca Melissa: é uma **página fraudulenta de e-commerce** que se apropria da **marca Melissa e do CNPJ da Grendene S.A.**, usa **fotos copiadas** de lojas reais e **preços irreais** para induzir o consumidor a um **checkout em domínio estrangeiro** (`compraonlinesegurada.org.ua`), onde coleta dados pessoais e gera um **PIX recebido por "BETRINHA LTDA"** — empresa sem qualquer relação com a Melissa. O perfil é compatível com o chamado **"golpe do PIX"** em e-commerce, em que o pagamento é feito e o produto não é entregue. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não comprar, não pagar o PIX e não fornecer dados pessoais** ao site nem ao checkout `compraonlinesegurada.org.ua`.
- Adquirir produtos Melissa apenas pelos **canais oficiais** da marca (site oficial e revendedores autorizados), desconfiando de **descontos muito acima do mercado** e de pagamento exclusivamente por PIX a pessoa/empresa diferente da loja.
- Se o PIX já foi pago: acionar imediatamente o **banco** e o mecanismo **MED** (Mecanismo Especial de Devolução) do PIX, reunir comprovantes (incluindo o nome do recebedor "BETRINHA LTDA") e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência.

Recomendações de mitigação / denúncia

- Reportar a página aos canais de abuse da **Vercel** (host do subdomínio) e da **Cloudflare** (que serve o checkout), e o domínio `compraonlinesegurada.org.ua` ao seu registrador (thehost.ua), anexando este laudo.
- Comunicar a **Grendene S.A. / Melissa** sobre o uso indevido da marca e do CNPJ, para as providências de propriedade industrial cabíveis, e reportar o recebedor PIX e a cobrança às instituições de pagamento envolvidas (**Treeal** e **ParadisePag**) pelos respectivos canais de prevenção a fraude.
- 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 site 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, Amazon AWS, Cloudflare, Hostinger) nem às instituições de pagamento (Treeal, ParadisePag) citados, meros intermediários.

— Fim do relatório —

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