RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

cestasbomdiaeamor.shop

Objeto investigado	cestasbomdiaeamor.shop — falsa loja de cestas de presente (gTLD .shop)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	17/07/2026 (RDAP, DNS, HTTP/TLS, geolocalização, análise do checkout e do PIX)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise de conteúdo · decodificação BR Code
Achado central	Loja falsa que CAPTURA dados de cartão de crédito e exfiltra dados via Telegram; PIX a recebedor alheio à loja
Classificação	**RISCO ALTO**
Emissão do laudo	17/07/2026 às 01:30

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **cestasbomdiaeamor.shop**, realizada em **17/07/2026** 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 (cadeia de custódia).

O domínio **está no ar** e entrega uma **loja virtual de "cestas de café da manhã, presentes e flores" em português** ("Cestas Bom Dia e Amor"), construída como página única estática. A vitrine é carregada de um arquivo `dados.json` e as **fotos dos produtos são "hotlinkadas" de outro domínio** (`cestasdeamorr.shop`), num padrão de sites replicados. O checkout coleta **nome, CPF, telefone e endereço completo** e oferece dois meios de pagamento: **PIX** e **cartão de crédito**.

Foram constatados **dois comportamentos graves no código do checkout**. Primeiro, ao escolher cartão, o formulário coleta **número, validade, CVV e nome do cartão** e os envia ao próprio servidor (`checkout.php?action=cartao`) — um comentário no código alega falsamente que um gateway "HyperCash" "nunca grava/loga esses dados". Segundo, o comprovante de pagamento e os dados do comprador (nome, telefone, endereço) são **enviados diretamente a um bot do Telegram** controlado pelo operador (token e `chat_id` embutidos no HTML). Somam-se a isso indícios clássicos de fraude: domínio **registrado há 7 dias**, **titular oculto**, **avaliações fabricadas** ("647 avaliações"), pixels de **Google Ads** compatíveis com captação por tráfego pago e **CNPJ falso no rodapé**.

No fluxo PIX, o código "copia e cola" foi decodificado (BR Code/EMV). O recebedor declarado é **"MADRIGAL PROV LTDA"** (Brasília/DF) e a cobrança é intermediada pelo gateway **MagenPay** (`pix.magenpay.io`); o identificador da cobrança aponta ainda para um **terceiro CNPJ** (MEI de Barueri/SP). **Nenhum** desses nomes corresponde à loja anunciada — o dinheiro **não vai para "Cestas Bom Dia e Amor"**, e sim para contas de terceiros por meio de um agregador de pagamentos.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: uma loja que **captura dados de cartão de crédito** e exfiltra dados pessoais para um canal privado (Telegram), com **recebedor de PIX alheio à loja**, identificação falsa e vitrine copiada, reúne o perfil típico de **golpe de comércio eletrônico com roubo de dados de pagamento (carding)**. Recomenda-se **não comprar, não pagar e, sobretudo, não digitar dados de cartão** (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 acesso direto a servidores de DNS (porta 53) estava indisponível no ambiente de coleta, as consultas de DNS foram feitas por **DNS-over-HTTPS** (resolvedor 1.1.1.1); o conteúdo HTTP/HTTPS foi coletado por requisição de visitante comum. O código "copia e cola" do PIX foi decodificado pelo padrão EMV/BR Code. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (registrador Name.com)	`rdap_raw.json`
DNS	DoH 1.1.1.1 (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_doh.txt` · `dns_dig.txt`
Conteúdo / cabeçalhos	HTTP e HTTPS (porta 80 e 443)	`corpo.html` · `http_headers.txt` · `http80_headers.txt`
Vitrine / checkout	Download de dados.json e checkout.html	`dados.json` · `checkout.html`

Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · ip-api.com · PTR	`geolocalizacao_ip.txt`
Pagamento (PIX)	Decodificação BR Code + payload da cobrança (JWS)	`pix_copiaecola.txt` · `pix_decodificado.txt` · `pix_payload_*`
Intermediário / recebedor	RDAP (magenpay.io) · consulta de CNPJ	`rdap_magenpay.json` · `cnpj_*.json`
Imagens / metadados	Download de assets · exiftool	`imagens/` · `metadata_exiftool.txt`

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

Domínio	cestasbomdiaeamor.shop (gTLD .shop)
Registro	**10/07/2026** · expira 10/07/2027 (validade de 1 ano)
Idade na coleta	**7 dias** — domínio recém-registrado
Titular	**Oculto** (RDAP expõe apenas o registrador)
Registrador	Name.com, Inc. (abuse@name.com)
Status	clientTransferProhibited
Servidores de nome	ns1 / ns2.brasil148-2547.com.br (revenda de hospedagem "Brasil148")
DNS — A	107.150.167.226 · sem AAAA · MX aponta para o próprio domínio · SPF declara o mesmo IP
www	CNAME para o domínio raiz (mesmo IP)
Hospedagem	AS53038 IDC19 Soluções em TI / Núcleo Brasil Servidores — Vinhedo/SP (Datacenter Ascenty)
PTR reverso	br.brasil148-2547.com.br
Cabeçalhos reveladores	"Servidor: Nucleo Brasil Servidores" · "Localizacao: Brasil148 - Ascenty - SP Brasil"
Certificado TLS	CN=cestasbomdiaeamor.shop · emissor Let's Encrypt YR2 (DV) · válido 10/07/2026–08/10/2026
Série / Fingerprint	0550E7D06E74682A…B844FDE4D9 · SHA-256 B8:5C:A1:0D:C2:2C:03:9F:ED:ED:51:3F:C7:A9:2D:D8…
Domínio das imagens	cestasdeamorr.shop (registro 11/06/2026, Hostinger/HostGator) — fotos servidas de 50.6.138.99 (Oracle/Bluehost)

Leitura técnica. Registro há apenas 7 dias, validade de 1 ano e titular oculto compõem um perfil de **baixa rastreabilidade do responsável**. A hospedagem é uma revenda nacional (Núcleo Brasil / "Brasil148") em datacenter em Vinhedo/SP. O certificado DV gratuito (Let's Encrypt) comprova apenas o controle do domínio, **não a identidade de qualquer empresa**. As fotos dos produtos são carregadas de um **segundo domínio .shop** (`cestasdeamorr.shop`), indicando reaproveitamento de acervo entre sites irmãos. Não se imputa conduta ao registrador nem aos provedores de hospedagem, meros intermediários de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site simula uma **loja de cestas de presente** (café da manhã, chocolates, flores, pelúcias). O checkout coleta dados pessoais e de entrega e oferece **PIX** e **cartão de crédito**. A análise do código do checkout revelou dois pontos críticos, descritos abaixo, além da decodificação do BR Code do PIX.

Aspecto	Constatação
Tipo de serviço	Loja virtual de cestas de presente / flores ("Cestas Bom Dia e Amor")
Tecnologia	Página única estática · vitrine em dados.json · imagens hotlinkadas de cestasdeamorr.shop
Dados pessoais coletados	Nome, CPF, telefone, endereço completo (CEP, rua, nº, bairro, cidade, complemento), nome/mensagem do destinatário
Captura de cartão	**SIM** — número, validade, CVV e nome do cartão enviados a checkout.php?action=cartao (comentário alega falsamente gateway "HyperCash" que "não grava/loga")
Exfiltração via Telegram	**SIM** — comprovante e dados do comprador enviados a api.telegram.org (bot token e chat_id embutidos no HTML)
Meio de pagamento (PIX)	PIX dinâmico intermediado por MagenPay (pix.magenpay.io — payload sobre AWS us-east-1 / gateway Kong)
Recebedor do PIX (BR Code)	**"MADRIGAL PROV LTDA" — Brasília/DF** (não corresponde à loja)
Identificador da cobrança	"Pagamento 65807341000119" → CNPJ 65.807.341/0001-19 (MEI Gabriel H. A. de Carvalho, Barueri/SP, aberto 20/03/2026) — **terceiro**, também alheio à loja
CNPJ no rodapé do site	**Falso/desviado** — 29.181.721/0001-27 = "Marcelo Borges" (situação INAPTA, atividade "condicionamento físico", São Paulo)
Avaliações	Fabricadas — "baseado em 647 avaliações", cards fixos com "Cliente verificado"
Rastreamento	Google Ads (AW-18316564208), GA4 (G-C9VEN66940) e Microsoft Clarity — compatível com captação por tráfego pago

Leitura técnica. O elemento mais grave é a **captura de dados de cartão de crédito**: o formulário coleta número, validade e CVV e os transmite ao servidor do próprio site, com um comentário no código que tenta tranquilizar a vítima ("gateway HyperCash que não grava/loga") — nome que não aparece em nenhum outro ponto e que não corresponde a intermediador identificável. Some-se a exfiltração de comprovante e dados pessoais para um **bot de Telegram** do operador. No PIX, os três nomes envolvidos (recebedor "MADRIGAL PROV LTDA", CNPJ da cobrança e CNPJ do rodapé) **são distintos entre si e nenhum é a loja anunciada** — padrão de ocultação do beneficiário final por meio de agregador de pagamentos. Não se imputa conduta ao intermediário MagenPay nem aos provedores de infraestrutura; descreve-se o fato técnico.
Imagens. As fotos de produto (WebP 1536×1024, sem qualquer metadado EXIF/câmera/autor) têm dimensões uniformes e padrão coerente com **geração por IA ou banco de imagens**, servidas de domínio irmão. Ver `imagens/metadata_exiftool.txt`.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Captura de dados de cartão de crédito (número, validade, CVV) enviados ao próprio servidor	`checkout.html`	ALTA
2	Exfiltração de comprovante e dados pessoais para bot de Telegram do operador	`checkout.html`	ALTA
3	Recebedor do PIX não corresponde à loja (MADRIGAL PROV LTDA); beneficiário oculto por agregador	`pix_decodificado.txt · pix_payload_decodificado.txt`	ALTA
4	CNPJ do rodapé falso/desviado (titular "Marcelo Borges", INAPTA, ramo alheio)	`corpo.html · cnpj_29181721000127.json`	ALTA

5	Domínio recém-registrado (7 dias), validade de 1 ano, titular oculto	`rdap_raw.json`	MÉDIA
6	Avaliações fabricadas ("647 avaliações", cards fixos "Cliente verificado")	`dados.json` · `corpo.html`	MÉDIA
7	Vitrine copiada / imagens hotlinkadas de domínio irmão (cestasdeamorr.shop)	`dados.json` · `rdap_cestasdeamorr.json`	MÉDIA
8	Pixels de Google Ads/GA4/Clarity compatíveis com captação por tráfego pago	`corpo.html`	BAIXA
9	Imagens sem metadados, dimensões uniformes (indício de IA/banco de imagens)	`metadata_exiftool.txt`	BAIXA

Síntese: 4 indicadores de severidade ALTA, 3 MÉDIA e 2 BAIXA. **Nenhum fator de legitimidade** (operador identificado e verificável, recebedor correspondente à loja, avaliações reais, histórico) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 17/07/2026, conclui-se que **cestasbomdiaeamor.shop** é uma **loja virtual falsa** voltada ao público brasileiro que, além de simular venda de cestas de presente, **captura dados de cartão de crédito** (número, validade e CVV) e **exfiltra dados pessoais e comprovantes para um bot de Telegram** do operador. O pagamento por PIX é encaminhado a **recebedores que não correspondem à loja** (recebedor "MADRIGAL PROV LTDA" e um terceiro CNPJ na cobrança), com o beneficiário final ocultado por agregador de pagamentos. O site apresenta ainda **CNPJ falso no rodapé**, **avaliações fabricadas**, **vitrine copiada** e **domínio registrado há 7 dias com titular oculto**. Classifica-se o caso como **RISCO ALTO** ao consumidor, com agravante de **roubo de dados de meio de pagamento**.

Recomendações ao consumidor / solicitante

- **Não comprar, não pagar por PIX e — sobretudo — não digitar dados de cartão de crédito** no site.
- Quem já **informou dados de cartão**: contatar imediatamente o banco/emissor, **bloquear e substituir o cartão** e contestar qualquer cobrança não reconhecida.
- Quem já **pagou por PIX**: acionar o banco e o mecanismo **MED** (Mecanismo Especial de Devolução) do PIX, reunir comprovantes e registrar Boletim de Ocorrência.
- Desconfiar de anúncios (Google, Instagram, WhatsApp) e preços muito abaixo do mercado que conduzam a `cestasbomdiaeamor.shop`.

Recomendações de mitigação / denúncia

- Reportar o domínio ao canal de **abuse do registrador Name.com** (abuse@name.com) e ao provedor de hospedagem (Núcleo Brasil Servidores / "Brasil148"), anexando este laudo, para retirada do ar.
- Comunicar o **gateway MagenPay** e os bancos dos recebedores identificados (recebedor "MADRIGAL PROV LTDA" e o CNPJ da cobrança) sobre o uso do serviço para intermediar loja fraudulenta.
- Registrar denúncia em **consumidor.gov.br** e, dado o roubo de dados de cartão, comunicar as bandeiras/banco emissor e a autoridade policial (delegacia de crimes cibernéticos).
- 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.