RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

latam-airlines-black.com

Objeto investigado	latam-airlines-black.com — site de "venda de passagens" que se passa pela LATAM Airlines
Natureza	Suspeita de phishing / fraude de marca (brand abuse) e golpe ao consumidor
Data da coleta	10/06/2026 (RDAP, DNS, HTTP/TLS, geo, crt.sh, urlscan.io, análise do anúncio)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · geolocalização · fontes públicas de reputação
Achado central	Site fraudulento imitando a LATAM, distribuído por Google Ads (malvertising) e com cloaking anti-análise
Classificação	**RISCO ALTO**
Emissão do laudo	10/06/2026 às 22:16

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **latam-airlines-black.com**, realizada em **10/06/2026** 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 hash SHA-256 calculado no momento da coleta.

O domínio **está no ar** e se apresenta como um site de **venda de passagens aéreas que imita a LATAM Airlines** — o próprio nome incorpora a marca "LATAM Airlines" e o produto "LATAM Black". O servidor (`openresty` + **PHP 8.1**) responde, mas aplica **cloaking**: entrega página **em branco** a requisições diretas e, a serviços de varredura (urlscan.io), exibiu uma **página-isca genérica** ("Beyond Hotel", um template não preenchido), enquanto direciona o conteúdo fraudulento da LATAM ao público-alvo. O site **geolocaliza o visitante por IP** (grava cookies `location`/`lastIp`) e funciona por **links de campanha** (`/?code=…`) que levam a páginas de "oferta de voos" (`/<uuid>/oferta-voos?…origin_code=…&destiny_code=…`).

A **distribuição se dá por anúncios pagos no Google (Google Ads / malvertising)**: o link examinado parte de um clique de anúncio (`googleadservices … gclid`) e passa por uma página intermediária em **beacons.ai/lattur** antes de chegar ao site falso — técnica que usa a marca LATAM para capturar vítimas em buscas por passagens. O domínio **já acumula 457 análises públicas no urlscan.io** (atividade contínua entre 17/05 e 09/06/2026), sinal de operação ativa e amplamente observada.

Trata-se de domínio **recém-registrado** (23/03/2026), com **titular oculto**, hospedado em nuvem (Google Cloud, São Paulo) e com infraestrutura de e-mail própria (Mailgun) — capaz de disparar falsas confirmações de reserva/cobrança. O conjunto é incompatível com um canal oficial da LATAM (cujo site legítimo é `latamairlines.com` / `latam.com`).

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: um site que **imita a LATAM**, é **impulsionado por anúncios pagos**, **esconde-se de ferramentas de análise** e vende "passagens" coletando dados e pagamento, reúne os indicadores típicos de **phishing / golpe de venda de passagens**. Recomenda-se **não comprar, não pagar e não fornecer dados**; usar apenas os canais oficiais da companhia (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; como o cliente curl não conduziu o corpo HTTP, os cabeçalhos foram coletados por requisição HTTP/1.1 bruta sobre TLS via `openssl s_client`. Por o site aplicar **cloaking** (corpo vazio para requisições diretas), o aspecto e o fluxo reais foram corroborados por **fontes públicas de reputação** (urlscan.io e crt.sh) e pela análise do **link de anúncio** fornecido. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (Verisign / .com — registrador GoDaddy)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Conteúdo / cabeçalhos	openssl s_client (HTTP/1.1 sobre TLS)	`headers_https.txt` · `raw_https_response.txt`
Certificado TLS	openssl s_client / x509	`ssl_cert.txt` · `ssl_raw.txt`
Geolocalização do IP	ipinfo.io · ip-api.com · PTR	`ipinfo_*.json` · `ipapi_*.json` · `ptr_reverse.txt`

Reputação / aparência	urlscan.io (scans, URLs, screenshots) · crt.sh	`urlscan*.json · crtsh.json · imagens/`
Distribuição (anúncio)	Análise do link Google Ads → beacons.ai	`headers_beacons.txt`

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

Domínio	latam-airlines-black.com (gTLD .com — Verisign)
Registro	**23/03/2026** · expira 23/03/2027 (validade de 1 ano)
Idade na coleta	**~11 semanas** — domínio recente
Titular	**Oculto** (privacidade; RDAP expõe só o registrador)
Registrador	GoDaddy.com, LLC
Status	clientDelete/Renew/Transfer/UpdateProhibited (travas padrão do registrador)
Servidores de nome	ns49 / ns50.domaincontrol.com (GoDaddy)
DNS — A	34.151.236.207 · sem AAAA · www = CNAME para o apex
E-mail (MX/SPF)	mxa / mxb.mailgun.org · TXT "v=spf1 include:mailgun.org ~all" (envio via Mailgun)
Hospedagem	AS396982 Google LLC — Google Cloud, região southamerica-east1
Geolocalização do IP	São Paulo / Brasil (datacenter; hosting: true)
PTR reverso	207.236.151.34.bc.googleusercontent.com
Servidor web	openresty · PHP/8.1.27 · grava cookies com geolocalização do visitante (location / lastIp)
Certificado TLS	CN=latam-airlines-black.com · Let's Encrypt YE2 (DV, ECDSA P-384) · válido 03/06–01/09/2026
Série / Fingerprint	059B087C09645BB2…58B5141 · SHA-256 BE:94:72:74:BE:7B:D3:86:53:92:6C:5A:5E:E8:7C:97…
Histórico (crt.sh)	12 emissões desde 24/03/2026 (GoDaddy + reemissões Let's Encrypt) — operação contínua
Reputação (urlscan.io)	**457 análises públicas** do domínio (atividade 17/05–09/06/2026)

Leitura técnica. Registro recente, validade de 1 ano e titular oculto compõem um perfil de **baixa rastreabilidade do responsável**. O certificado DV gratuito comprova apenas o controle do domínio, **não vínculo com a LATAM**. O nome que embute a marca, a hospedagem em nuvem genérica e o e-mail via Mailgun são incompatíveis com um canal corporativo da companhia. Não se imputa conduta ao registrador (GoDaddy), ao provedor de hospedagem (Google Cloud), ao serviço de e-mail (Mailgun), à plataforma de links (Beacons) nem à rede de anúncios (Google Ads) — meros intermediários de infraestrutura/serviço.

4. Natureza do Site, Distribuição (Anúncio) e Dados Coletados

O domínio reproduz a identidade da **LATAM Airlines** e do produto "LATAM Black" para vender **passagens aéreas**. As URLs observadas em fontes públicas revelam o fluxo: **links de campanha** (`/?code=<nome>`) e páginas de **oferta de voos** (`/<uuid>/oferta-voos?classType=economy&adults=1&kids=0&babies=0&origin_code=THE&destiny_code=FLL&departureDate=…&arrivalDate=…`) que simulam uma busca real de passagens (origem/destino por código IATA, datas e passageiros). O site **esconde-se de análise**: a serviços de varredura entregou uma **isca neutra** ("Beyond Hotel", template de reservas não preenchido), enquanto reserva o conteúdo LATAM ao tráfego-alvo — e **geolocaliza o visitante por IP** (cookies `location` e `lastIp`).

Aspecto	Constatação
Marca imitada	LATAM Airlines / "LATAM Black" — embutida no próprio nome do domínio (brand abuse)
Site oficial legítimo	latamairlines.com / latam.com — este domínio NÃO pertence à companhia
Tipo de golpe	Venda de passagens falsas / phishing (rota /oferta-voos com busca de voos simulada)
Distribuição	Google Ads (malvertising; link com gclid) → intermediário beacons.ai/lattur → site falso
Cloaking / evasão	**Sim** — corpo vazio a requisições diretas; isca "Beyond Hotel" a scanners; geofencing por IP
Infra de e-mail	Mailgun (MX/SPF) — capacidade de enviar falsas confirmações de reserva/cobrança
Dados / pagamento	Fluxo de compra de passagem → coleta de dados do passageiro (nome, CPF, contato) e pagamento (PIX/cartão) — *inferência do fluxo; não confirmado por captura direta devido ao cloaking*
Reputação pública	457 análises no urlscan.io; certificados reemitidos com frequência (operação ativa)

Leitura técnica. A combinação de **imitação de marca no domínio**, **impulsionamento por anúncios pagos**, **cloaking anti-análise** e **página de venda de passagens** caracteriza um esquema de phishing/golpe ao consumidor. O uso de uma página intermediária (beacons.ai) e de geofencing serve para escapar da detecção das plataformas de anúncio e de varredura. A coleta de dados pessoais e de pagamento é a finalidade esperada do fluxo de "compra"; registra-se como **inferência**, pois o cloaking impediu a captura direta do checkout — distingue-se aqui inferência de prova. Não se imputa conduta aos provedores citados.
Imagens. As capturas preservadas em `imagens/` são **screenshots públicos do urlscan.io** (não do próprio site), úteis para evidenciar o cloaking: mostram a isca "Beyond Hotel" exibida a scanners. Não contêm metadados EXIF/GPS relevantes.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Domínio imita a marca LATAM Airlines / "LATAM Black" (brand abuse)	`RDAP · nome do domínio`	ALTA
2	Distribuído por Google Ads (malvertising) via beacons.ai/lattur	`link de anúncio (gclid)`	ALTA
3	Cloaking anti-análise: isca "Beyond Hotel" a scanners; geofencing por IP	`urlscan.io · headers_https.txt`	ALTA
4	Página de venda de passagens (/oferta-voos) coletando dados/pagamento	`urlscan.io (URLs)`	ALTA
5	457 análises públicas no urlscan.io (amplamente observado)	`urlscan.json`	ALTA
6	Domínio recém-registrado (~11 semanas), validade de 1 ano	`RDAP — 23/03/2026`	MÉDIA
7	Titular oculto (privacidade de registro)	`RDAP — só registrador`	MÉDIA
8	Infra de e-mail Mailgun (falsas confirmações de reserva/cobrança)	`dns_records.txt`	MÉDIA

9	Reemissões frequentes de certificado TLS (operação ativa)	`crtsh.json`	BAIXA

Síntese: 5 indicadores de severidade ALTA, 3 MÉDIA e 1 BAIXA. **Nenhum fator de legitimidade** (vínculo verificável com a LATAM, identificação do operador, canal oficial) foi constatado.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em 10/06/2026, conclui-se que **latam-airlines-black.com** é um **site fraudulento que se passa pela LATAM Airlines** para vender "passagens", **distribuído por anúncios pagos no Google** (via intermediário beacons.ai) e dotado de **cloaking** para escapar de análise. Recém-registrado, de titular oculto e sem qualquer vínculo verificável com a companhia, reúne os indicadores típicos de **phishing / golpe de venda de passagens**. Classifica-se o caso como **RISCO ALTO** ao consumidor.

Recomendações ao consumidor / solicitante

- **Não comprar, não pagar e não fornecer dados** (nome, CPF, cartão, PIX) neste site; comprar passagens apenas pelos canais oficiais (`latam.com` / app oficial) ou agências reconhecidas.
- Desconfiar de **anúncios e links patrocinados** nos resultados de busca e em redes sociais que prometam passagens com desconto — conferir sempre o domínio antes de clicar.
- Se já houve pagamento: acionar o banco e o **MED** do PIX (ou o estorno/contestação no cartão), reunir comprovantes e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência.

Recomendações de mitigação / denúncia

- Denunciar o anúncio ao **Google Ads** (canal de denúncia de anúncios) e o site ao **Google Safe Browsing**; reportar aos canais de abuse do **GoDaddy** (registrador), do **Google Cloud** (hospedagem), do **Mailgun** (e-mail) e do **Beacons** (página intermediária), anexando este laudo.
- Comunicar a **LATAM Airlines** (uso indevido de marca) para acionamento jurídico e takedown.
- 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, de e-mail, de links e de anúncios citados, que figuram como intermediários.

— Fim do relatório —

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