RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, forense e de risco de fraude do domínio

claro-faturas.lat

Objeto investigado	claro-faturas.lat
Natureza	Suspeita de phishing / falsificação de identidade da operadora Claro Brasil
Data da coleta	26/05/2026 — 03:49 a 04:00 UTC (00:49–01:00 BRT)
Métodos	OSINT passivo · RDAP · DNS · análise de cabeçalhos HTTP · TLS · arquivo público urlscan.io
Emissão do laudo	26/05/2026 às 01:10

1. Sumário Executivo

Este relatório documenta a investigação técnica do sítio eletrônico **https://claro-faturas.lat**, que se apresenta ao público como "Central de Pagamentos · Claro" — uma página de consulta e quitação de faturas em nome da operadora brasileira **Claro**. A coleta de evidências foi realizada em 26/05/2026 por técnicas de OSINT (inteligência de fontes abertas) e análise forense passiva, sem qualquer interação intrusiva com a infraestrutura-alvo.

A análise identificou um **conjunto convergente e inequívoco de indicadores de phishing**: o domínio foi registrado há apenas **~2 meses**, no TLD *.lat* (Latino-América) — incompatível com a Claro Brasil, que opera oficialmente sob *claro.com.br*; a página reproduz a identidade visual e a marca registrada da Claro para coletar o número de telefone do consumidor; e o domínio se encontra **simultaneamente sinalizado pela Cloudflare como "Suspected Phishing"** e **suspenso pelo registro do TLD .lat (status "server hold")**. Foi localizado, ainda, um **domínio irmão (claro-faturas.com) registrado pelo mesmo registrador**, com a mesma infraestrutura, conteúdo equivalente em escaneamento histórico e atualmente "sanitizado" para evitar takedown.

CLASSIFICAÇÃO DE RISCO	ALTO RISCO — PHISHING CONFIRMADO POR TERCEIROS

A classificação é sustentada por **dois sinais externos independentes de confirmação**: a rotulagem do domínio como "Suspected Phishing" pela rede da Cloudflare (que atende as requisições à página) e a aplicação do status de bloqueio *server hold* pelo registro do TLD .lat (CentralNic) — ambos consistentes com o quadro fático descrito nas seções seguintes. Recomenda-se enfaticamente que consumidores **não informem o número de telefone, dados pessoais ou paguem qualquer "fatura"** no endereço investigado, e que o domínio irmão claro-faturas.com seja igualmente tratado como suspeito até comprovação em contrário.

2. Metodologia e Cadeia de Custódia

A investigação seguiu o princípio da **preservação probatória**: todas as respostas de rede e os artefatos obtidos foram salvos em arquivo no momento da coleta e tiveram seu valor de resumo criptográfico (hash SHA-256) calculado, permitindo verificação de integridade a qualquer tempo. Nenhuma técnica intrusiva, de exploração de vulnerabilidade ou de engenharia reversa de servidor foi empregada — apenas requisições equivalentes às de um visitante comum e consultas a bases públicas (RDAP, DNS, urlscan.io, ipinfo.io, RIPE).

Observação metodológica relevante: na data desta investigação, o domínio **claro-faturas.lat já estava sob bloqueio** em dois pontos da cadeia — pela Cloudflare (que devolve a página "Suspected Phishing") e pelo registro do TLD .lat (que removeu sua delegação NS, gerando NXDOMAIN para resolvers públicos). Por essa razão, a análise do conteúdo original foi conduzida a partir de **arquivo público preservado pela urlscan.io em 23/03/2026** (5 dias após o registro do domínio), com captura de tela, dados da resposta e cabeçalhos.

Etapa	Técnica / ferramenta	Evidência preservada
Registro do domínio	RDAP — CentralNic (registry .lat)	`rdap_raw.json`
Infraestrutura DNS	dig — resolver público + NS autoritativos	`dns_claro-faturas.lat.txt`
Cabeçalhos e corpo HTTP/HTTPS	curl — com --resolve para o IP da origem	`headers_https.txt` · `corpo_https.html` `headers_http.txt` · `corpo_http.html`
Certificado TLS	openssl s_client / x509	`ssl_cert.txt`

Geolocalização do IP / ASN	ipinfo.io · ip-api.com · whois.cymru · RIPE	`ipinfo.json` · `ipapi.json` `ip_geolocalizacao.txt`
Conteúdo original (arquivo)	urlscan.io — escaneamento de 23/03/2026	`urlscan_search.json` `urlscan_screenshot_2026-03-23.png`
Domínio irmão (claro-faturas.com)	RDAP Verisign · curl · urlscan.io	`rdap_claro-faturas.com.json` `corpo/headers/js_claro-faturas.com`

Todos os artefatos estão na subpasta **evidencias/** e seus hashes constam do Anexo A (Manifesto de Integridade). A captura de tela do conteúdo original e o preview do domínio irmão estão na subpasta **imagens/**. O fuso horário de referência é UTC; conversões para o horário de Brasília (BRT, UTC–3) são indicadas quando aplicável.

3. Identificação do Domínio (RDAP)

Os dados a seguir foram obtidos junto ao operador do registro do TLD **.lat** (CentralNic) pelo protocolo RDAP. O nome do titular ("registrant") não é divulgado pelo registro — política comum para esse TLD — mas o registrador, a data de registro, o status atual do domínio e os servidores de nome são informações públicas.

Domínio	claro-faturas.lat
Handle do registro	D628381812-CNIC
Data de registro	18/03/2026 22:54:58 UTC
Data de expiração	18/03/2027 23:59:59 UTC
Última alteração	18/05/2026 18:47:06 UTC — coincide com a aplicação do bloqueio
Idade do domínio	~2 meses na data da coleta — **domínio recente**
Período contratado	1 (um) ano — o mínimo possível
Registrador (Registrar)	Dynadot LLC (IANA ID 472)
Contato de abuso	abuse@dynadot.com · +1.650.262.0100
Titular / Registrant	Não divulgado pelo registro .lat
DNSSEC	Não assinado (delegationSigned: false)
Servidores de nome	ashton.ns.cloudflare.com · summer.ns.cloudflare.com
Status EPP	**server hold** · clientTransferProhibited

Leitura técnica. O status *server hold* indica que o **próprio registro do TLD** aplicou suspensão administrativa ao domínio — concretamente, removeu sua delegação NS da zona *.lat*. Isso faz com que resolvers DNS públicos retornem NXDOMAIN para o nome, embora os servidores Cloudflare ainda contenham a zona (Seção 4). A data da última alteração no registro (18/05/2026) coincide com a aplicação do bloqueio. A combinação *período mínimo (1 ano) + registro recente + bloqueio do registry* é altamente consistente com a operação de um domínio descartável, usado por algumas semanas até ser denunciado e substituído por outro do mesmo padrão — como, de fato, ocorre com o domínio irmão analisado na Seção 11.

4. Infraestrutura de DNS

A consulta a um resolver recursivo público (Google 8.8.8.8) retorna **NXDOMAIN** — efeito direto do status *server hold* aplicado pelo registro do TLD .lat. A consulta diretamente aos servidores autoritativos (Cloudflare), porém, ainda devolve a zona configurada pelo operador do domínio, expondo o IP de origem para o qual o site estava apontado:

Origem da resposta	Registro	Valor	Observação
Resolver público 8.8.8.8	NS / SOA / A	`NXDOMAIN`	Registry retirou a delegação NS por *server hold*
NS autoritativo (Cloudflare)	A	`185.158.133.1`	IP da plataforma **Lovable.dev** (Seção 5)
NS autoritativo (Cloudflare)	AAAA	— (ausente)	Sem IPv6
NS autoritativo (Cloudflare)	NS	`ashton.ns.cloudflare.com` `summer.ns.cloudflare.com`	DNS gerenciado pela Cloudflare
NS autoritativo (Cloudflare)	MX	— (ausente)	Domínio não recebe e-mail — sem canal de contato por correio eletrônico

NS autoritativo (Cloudflare)	TXT / SPF	— (ausente)	Sem políticas de e-mail; nenhuma verificação de propriedade
NS autoritativo (Cloudflare)	SOA	`ashton.ns.cloudflare.com (serial 2404457107)`	—
NS autoritativo (Cloudflare)	www	`– (sem registro próprio)`	Apenas o apex foi configurado

Leitura técnica. A inexistência de registros MX e TXT/SPF confirma que o domínio nunca foi operado para correio eletrônico — uma operadora real de telefonia/Internet jamais dispensaria e-mail corporativo associado a uma "central de pagamentos". A discrepância entre NXDOMAIN (resolvers públicos) e a zona ainda viva nos NS autoritativos é típica de domínios suspensos pelo registry: o operador do domínio é apenas desconectado do DNS global, mas a configuração na Cloudflare permanece intacta — o que permitiria reativação imediata caso o bloqueio fosse revertido.

5. Hospedagem e Geolocalização do Servidor

Endereço IP da origem	185.158.133.1
Sistema autônomo (ASN)	AS13335 — Cloudflare, Inc.
Prefixo BGP	185.158.133.0/24 (alocado em 2016-07-05, registro RIPE NCC)
Tipo de IP	**Anycast** Cloudflare — geolocalização varia por base de dados (ipinfo.io: Polônia; ip-api.com: Frankfurt/Alemanha)
DNS reverso (PTR)	`lovable-app-cd-1-4.p.l5e.io`
Plataforma de hospedagem	**Lovable.dev** — construtor de aplicações web por IA (no-code)
Servidor HTTP	cloudflare (proxy reverso à frente da plataforma)

Achado relevante — site construído em plataforma no-code de IA. O DNS reverso do IP que recebia as requisições resolve para **lovable-app-cd-1-4.p.l5e.io**, infraestrutura da plataforma **Lovable.dev** — serviço comercial de criação de aplicações web pela conversação com modelos de linguagem ("vibe coding"). Esse tipo de plataforma permite que um operador, em horas, publique réplicas verossímeis da identidade visual de marcas conhecidas, sem qualquer codificação manual, e a baixíssimo custo. Não se imputa aqui conduta ilícita à Lovable nem à Cloudflare — são provedores de infraestrutura; o ponto relevante é que **uma "central de pagamentos" de uma operadora de telecomunicações brasileira não seria, em hipótese alguma, publicada num construtor de IA hospedado em anycast multinacional**, e essa escolha indica fortemente uma operação descartável de fachada.

Incompatibilidade institucional. A Claro S.A. (Claro Brasil) opera oficialmente sob o domínio **claro.com.br** — registrado junto ao Registro.br (NIC.br) — e nunca dispôs de subdomínio nem domínio paralelo no TLD **.lat**. O TLD .lat foi delegado em 2015 para o público latino-americano e seu uso por uma operadora estabelecida sob .com.br não tem justificativa operacional alguma. A escolha do TLD .lat compõe a **fachada de marca** e não corresponde a qualquer canal real da empresa imitada.

6. Certificado TLS / HTTPS

Titular (Subject)	CN = claro-faturas.lat
Emissor (Issuer)	Google Trust Services — autoridade "WE1" (C = US)
Tipo de validação	DV — Domain Validation (apenas controle sobre o domínio)
Algoritmo de assinatura	ecdsa-with-SHA256 (chave EC P-256)
Válido de	17/05/2026 03:45:18 UTC
Válido até	15/08/2026 04:43:59 UTC
Número de série	ED:C4:30:B9:8F:4B:F8:EA:13:3E:07:76:31:25:7B:DD
Fingerprint SHA-256	39:14:5F:7D:47:13:D0:1A:D1:32:91:85:79:F4:50:15: 70:97:66:AA:75:8F:5E:83:1C:63:14:FB:8A:DD:A4:C4
Subject Alternative Name	DNS:claro-faturas.lat (somente)

Leitura técnica. O certificado é válido e a conexão HTTPS é legítima do ponto de vista criptográfico — porém é um certificado **gratuito do tipo DV**, emitido pela Google Trust Services e provisionado automaticamente pela infraestrutura Cloudflare/Lovable. DV apenas comprova o controle sobre o domínio e **não atesta a identidade de qualquer pessoa jurídica**; o "cadeado" do navegador, portanto, não pode ser lido pelo consumidor como garantia de idoneidade do estabelecimento. Observe-se que esta é a **segunda emissão** conhecida — a urlscan.io registrou em 23/03/2026 um certificado anterior com validade desde 18/03/2026 (data do registro), substituído após o ciclo de 90 dias.

7. Resposta HTTP — Bloqueio Ativo pela Cloudflare

Na data desta coleta (26/05/2026), as requisições HTTPS e HTTP à página claro-faturas.lat são interceptadas pela Cloudflare e **respondidas com HTTP 403 e a página institucional "Suspected Phishing"**. Isso significa que a própria rede de entrega de conteúdo que serve o site classificou-o como golpe e interrompeu a entrega do conteúdo original ao público.

Método	Resposta	Cabeçalhos relevantes

GET https://claro-faturas.lat/	**HTTP/2 403** — "Suspected Phishing | Cloudflare"	`server: cloudflare`
		`cf-ray: a019d49b29f38aef-GIG`
		`content-type: text/html; charset=utf-8`
		`x-frame-options: SAMEORIGIN`
		`referrer-policy: same-origin`

GET http://claro-faturas.lat/	**HTTP/1.1 403 Forbidden** — mesma página	`server: cloudflare` `cf-ray: a019d4fe5b646f01-GIG`

O corpo HTML retornado pela Cloudflare apresenta literalmente os seguintes textos (extraídos do arquivo `evidencias/corpo_https.html`):

> "**Suspected Phishing**
> This website has been reported for potential phishing. Phishing is when a site attempts to steal sensitive information by falsely presenting as a safe source."

Leitura técnica. O bloqueio pela Cloudflare é um **sinal externo de validação** praticamente equivalente, no domínio técnico, a uma denúncia formal: o operador da CDN *tem* visibilidade do tráfego real e *classificou* o conteúdo, independentemente do que veria um analista humano. Quando esse bloqueio coexiste com a suspensão no registry do TLD (Seção 3), há dupla confirmação externa do quadro de phishing. A página de bloqueio também revela, no canto inferior, o *Ray ID* da requisição — útil para eventual subpoena ou para reportes de incidente.

8. Conteúdo Original da Página (registro de arquivo)

Como o conteúdo do site está hoje substituído pela página de bloqueio da Cloudflare (Seção 7), a análise do que era originalmente apresentado ao visitante foi feita a partir de **registro público preservado pela urlscan.io** em **23/03/2026 13:31 UTC** — 5 dias após o registro do domínio. O escaneamento manual capturou, na ocasião, o HTML, o screenshot e o conjunto de requisições, retornando título da página, IP atendente (o mesmo 185.158.133.1 atual), país declarado pelo geo-IP (DE), tempo de validade do TLS (90 dias) e idade do domínio (4 dias).

Identificador urlscan	019d1ae4-6d13-7117-b908-a55c455e3e2a
Data do escaneamento	23/03/2026 13:31:17 UTC
Idade do domínio na ocasião	4 dias
URL escaneada	http://claro-faturas.lat/ (com redirecionamento HTTPS)
Título HTML capturado	**"Claro Faturas Pagamentos"**
IP atendente	185.158.133.1 (idêntico ao atual)
Idioma declarado	pt (português)
Status HTTP na ocasião	200 (página servida normalmente)
Captura de tela	imagens/urlscan_screenshot_2026-03-23.png

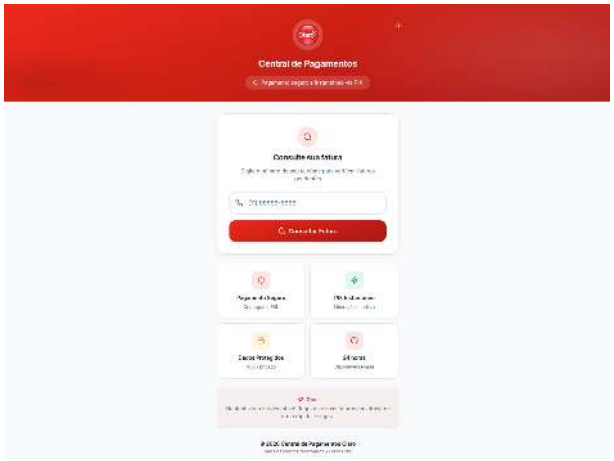

Figura 1 — Captura da página claro-faturas.lat preservada pela urlscan.io em 23/03/2026. Reproduz a identidade visual da operadora Claro (logo vermelho circular, paleta vermelha em degradê), título "Central de Pagamentos · Pagamento seguro e instantâneo via PIX", um único formulário pedindo o **número de telefone** do consumidor ("(11) 99999-9999") para "Consultar Fatura", quatro selos de confiança ("Pagamento Seguro · Criptografia SSL", "PIX Instantâneo · Liberação imediata", "Dados Protegidos · 100% privado", "24 horas · Disponível sempre") e o rodapé "© 2026 Central de Pagamentos Claro · Todos os direitos reservados · Claro Brasil".

Leitura técnica. O conteúdo capturado é um clone visual de "central de pagamentos" da Claro com **uma única função aparente**: capturar o número de telefone do visitante sob a desculpa de "consultar fatura". O fluxo subsequente — ausente no escaneamento estático — é tipicamente o seguinte em golpes desse tipo: (i) o visitante informa o telefone; (ii) o site exibe um "valor de fatura em atraso"; (iii) gera-se um código PIX "copia e cola" cujo recebedor é uma pessoa física ou empresa de fachada, completamente desvinculada da Claro. Os "selos de confiança" reproduzidos na página (criptografia, privacidade, 24 horas) são **elementos puramente decorativos, sem qualquer correspondência técnica** — não há autoridade certificadora, auditor ou política de privacidade verificáveis vinculados àqueles termos.

9. Padrão de Fraude — Imitação de Marca

O caso reúne todos os elementos clássicos do **phishing por imitação de marca de operadora brasileira**, gênero amplamente documentado pelas equipes de resposta a incidentes brasileiras (CERT.br, SaferNet) e pela própria Claro em seus canais oficiais. O padrão é o seguinte:

Elemento do golpe	Materialização nesta investigação
Domínio look-alike	claro-faturas.lat — combina a marca registrada "Claro" com uma palavra de função ("faturas") em um TLD descartável. A operadora real opera **claro.com.br**; nunca utilizou ".lat".
Reprodução da identidade visual	Logo circular vermelho, paleta de cores oficial, tipografia coerente, ícones e nomenclatura ("Central de Pagamentos", "Fatura") que evocam o portal genuíno.
Ponto de captura do dado	Único campo do formulário: **número de telefone celular** (placeholder "(11) 99999-9999"). É o vetor primário de fraude — uma vez capturado, alimenta um banco de números reais brasileiros e habilita o passo seguinte.
Modal de pagamento	"Pagamento seguro e instantâneo via PIX" anunciado em destaque — exatamente o canal sem rastreabilidade nem chargeback que os esquemas preferem.
Selos de confiança fabricados	"Criptografia SSL · Dados Protegidos · 100% privado · 24 horas Disponível sempre" — elementos decorativos, não verificáveis.
Uso de marca sem autorização	Rodapé "© 2026 Central de Pagamentos Claro · Todos os direitos reservados · Claro Brasil" — utilização indevida do nome empresarial alheio, configurando, em tese, infração de marca registrada (Lei 9.279/1996).
Infraestrutura descartável	Site construído em plataforma no-code de IA (Lovable.dev), domínio contratado pelo prazo mínimo (1 ano) — operação projetada para sobreviver semanas até takedown.
Domínio irmão paralelo	claro-faturas.com (registrado 2 meses antes, mesmo registrador, mesma infraestrutura) ainda ativo, atualmente em "modo sanitizado" — ver Seção 11.

Leitura técnica. A captura inicial do número de telefone é, em si, valiosa: serve para enriquecer listas usadas em campanhas de SMS phishing ("smishing") e ligações fraudulentas, e permite ao operador do golpe selecionar quem prossegue para a etapa de pagamento (filtrando números obviamente inválidos ou de pesquisadores). O par "telefone + fatura PIX" é a combinação típica de uma **operação dirigida ao consumidor brasileiro**.

10. Indicadores de Fraude (IoF)

A tabela consolida os indicadores objetivos identificados. Cada um isoladamente já seria preocupante; a **convergência** com dois sinais externos independentes de confirmação (bloqueio Cloudflare e suspensão pelo registry) torna a classificação inequívoca.

#	Indicador	Evidência	Severidade
1	Cloudflare devolve a página "Suspected Phishing" para o domínio	`HTTP 403 + corpo de bloqueio Cloudflare`	ALTA
2	Registro do TLD .lat aplicou status "server hold" (suspensão)	`RDAP — status: ["server hold","client transfer prohibited"]`	ALTA
3	Uso indevido da marca "Claro" no nome de domínio e no conteúdo	`claro-faturas.lat + rodapé "Claro Brasil"`	ALTA
4	Domínio recém-registrado (~2 meses), pelo prazo mínimo (1 ano)	`RDAP — registro 18/03/2026; expira 18/03/2027`	ALTA
5	Pagamento anunciado exclusivamente via PIX	`Página: "Pagamento seguro e instantâneo via PIX"`	ALTA
6	Domínio irmão (claro-faturas.com) com mesmo padrão e infraestrutura	`RDAP Verisign + escaneamentos urlscan.io 01/2026 e 03/2026`	ALTA
7	TLD .lat incompatível com operadora brasileira (claro.com.br oficial)	`TLD .lat (Latino-América); Claro nunca operou ".lat"`	ALTA
8	Site construído em plataforma no-code de IA (Lovable.dev)	`PTR lovable-app-cd-1-4.p.l5e.io / AS Cloudflare`	MÉDIA
9	Coleta de telefone como ponto inicial de captura	`Campo único do formulário: "(11) 99999-9999"`	MÉDIA
10	Selos de confiança fabricados (SSL, privacidade, 24 horas)	`Bloco visual da página (Figura 1)`	MÉDIA
11	Ausência de MX / SPF — domínio sem e-mail corporativo	`Consulta DNS aos NS autoritativos`	MÉDIA
12	Titular não divulgado e registrar offshore (Dynadot, EUA)	`RDAP — entity registrar`	BAIXA

Síntese: 7 indicadores de severidade ALTA, 4 de severidade MÉDIA e 1 de severidade BAIXA. Destacam-se os dois primeiros — **são confirmações externas, vindas do próprio operador da rede de entrega (Cloudflare) e do operador do registro do TLD (CentralNic)** — que, no domínio técnico, equivalem a declarações formais de tratamento como phishing.

11. Domínio Irmão e Operação Continuada (claro-faturas.com)

Durante a investigação foi identificado, no escaneamento histórico da urlscan.io, um **domínio irmão** com o mesmo padrão de nome, mesma infraestrutura e conteúdo equivalente. Trata-se de **claro-faturas.com**, registrado no mesmo registrador (Dynadot), apontando para o mesmo cluster Cloudflare e Lovable.dev:

Domínio irmão	claro-faturas.com
Data de registro	20/01/2026 (anterior em ~2 meses ao domínio .lat)
Última alteração	21/03/2026
Expiração	20/01/2027
Registrador	Dynadot Inc. (mesmo do .lat)
Nameservers	ashton.ns.cloudflare.com · summer.ns.cloudflare.com (idênticos ao .lat)
Status RDAP atual	client transfer prohibited (ativo, sem server hold)
Resposta HTTP atual	HTTP/2 200 — servida normalmente (não bloqueada pela Cloudflare)
Título HTML atual	"Guia Informativo — Segunda Via de Fatura Claro"
Posicionamento textual atual	Página descreve-se como "guia independente, sem vínculo com a Claro"

Histórico do conteúdo do domínio irmão (urlscan.io):

Data	Título HTML	IP atendente
20/01/2026 23:34 UTC	"Central de Pagamentos Claro | Pague sua Fatura"	`216.198.79.65 (Vercel)`
20/01/2026 23:36 UTC	"Central de Pagamentos Claro | Pague sua Fatura"	`216.198.79.65 (Vercel)`
20/01/2026 23:58 UTC	"Central de Pagamentos Claro | Pague sua Fatura"	`216.198.79.65 (Vercel)`
16/03/2026 21:52 UTC	"Claro Faturas Pagamentos"	`185.158.133.1 (Cloudflare/Lovable)`
26/05/2026 (esta coleta)	"Guia Informativo — Segunda Via de Fatura Claro"	`Cloudflare/Lovable`

Leitura técnica. A linha do tempo mostra a evolução clássica de uma operação que tenta escapar de takedown: primeiro publicada em **Vercel** (janeiro/2026) com título de pagamento direto, depois migrada para **Cloudflare/Lovable** (março/2026) com o mesmo posicionamento, e finalmente — depois de o domínio .lat do mesmo operador ter sido suspenso — **"sanitizada" para um discurso de "guia independente"**. O front-end atual de claro-faturas.com é tecnicamente uma *single-page application* em React (bundle *index-nYeRGlIK.js* de 332 KB) cujo HTML inicial contém apenas a estrutura mínima e um *JSON-LD* com `"publisher": "PROMEX COMERCIO, IMPORTACAO E EXPORTACAO LTDA"`. A inserção de uma razão social genérica no *schema.org*, sem qualquer aviso visível ao usuário sobre a propriedade do site, é um sinal adicional de tentativa de aparentar legitimidade sem assumir responsabilidade pública.

A sanitização não descaracteriza o quadro: **(i)** a apresentação inicial do domínio era de phishing direto (confirmado por urlscan); **(ii)** o domínio segue ativo e em mãos do mesmo operador; **(iii)** rotas alternativas (subdomínios, paths específicos, redirecionamentos vindos de SMS) podem continuar exibindo o conteúdo original a vítimas escolhidas, sem que isso apareça no acesso pela página raiz; **(iv)** o operador pode reverter o conteúdo a qualquer momento, dado que controla a aplicação no Lovable.dev. Recomenda-se monitorar o domínio.

12. Conclusão Técnica

Com base nas evidências coletadas e preservadas em 26/05/2026, conclui-se que o sítio **claro-faturas.lat** consiste em **página de phishing** que imita a operadora brasileira Claro com a finalidade aparente de capturar o número de telefone de consumidores e, em fluxo subsequente, induzi-los ao pagamento via PIX de "faturas" inexistentes — em proveito de terceiros sem qualquer vínculo com a Claro S.A.

A análise reúne **doze indicadores objetivos**, dos quais dois são **confirmações externas independentes** de tratamento como phishing: (a) a rede Cloudflare, que serve as requisições ao domínio, responde com a página institucional "Suspected Phishing" (HTTP 403); e (b) o registro do TLD .lat aplicou ao domínio o status EPP "server hold", retirando sua delegação de DNS na zona global. Some-se a isso a **identificação de um domínio irmão (claro-faturas.com)** sob o mesmo registrador e infraestrutura, historicamente operado com idêntico conteúdo e atualmente "sanitizado" para evitar nova suspensão — sinal de que se trata de operação continuada, não isolada.

Registre-se que a validação criptográfica do HTTPS (certificado Google Trust Services) é legítima, porém irrelevante para a aferição de idoneidade: trata-se de certificado gratuito de validação de domínio, provisionado pela própria plataforma de hospedagem (Lovable.dev) e que não atesta a identidade de qualquer pessoa jurídica. Não há, em nenhum dos artefatos coletados, identificação de uma empresa real responsável pelo domínio — o titular permanece oculto pela política de privacidade do registro .lat, e a única razão social que aparece no domínio irmão (PROMEX COMERCIO IMPORTACAO E EXPORTACAO LTDA) consta apenas dentro do código-fonte da página atual, sem qualquer divulgação ao usuário.

Ressalva metodológica: este laudo baseia-se em fontes abertas e na análise de conteúdo público e arquivos públicos preservados (urlscan.io) na data indicada. A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial ou judicial.

13. Recomendações

Para o consumidor / solicitante

- **Não informar o número de telefone** nem qualquer dado pessoal em claro-faturas.lat, em claro-faturas.com ou em variantes do mesmo padrão.
- **Não pagar qualquer "fatura" via PIX** originária desses endereços. A Claro emite cobrança exclusivamente pelos canais oficiais (app Minha Claro Residencial / Minha Claro Móvel, claro.com.br e boletos com código de barras vinculados ao CNPJ da Claro S.A.).
- Caso já tenha informado o telefone, considerar o número exposto e atentar-se a contatos subsequentes por SMS ou ligação que peçam dados adicionais ou pagamento.
- Caso já tenha pago, acionar imediatamente o banco e solicitar o **Mecanismo Especial de Devolução (MED)** do PIX, registrando contestação de fraude.
- Registrar Boletim de Ocorrência (delegacia física ou eletrônica) e reunir comprovantes (prints, recibos PIX, mensagens SMS/WhatsApp que levaram ao site).
- Denunciar o site à **SaferNet Brasil** (new.safernet.org.br) e à própria **Claro** (canal de denúncia de fraudes em claro.com.br/seguranca).

Para responsáveis técnicos / takedown

- Reportar abuso ao registrador **Dynadot LLC** (abuse@dynadot.com) — para o domínio irmão **claro-faturas.com**, que segue ativo. Anexar este laudo.
- Reportar à **Cloudflare** (abuse@cloudflare.com / cloudflare.com/abuse) — operadora da CDN; já trata o domínio .lat como phishing, mas o .com segue servido por sua infraestrutura.
- Reportar ao **provedor da aplicação** — Lovable.dev (abuse@lovable.dev) — solicitando a remoção do projeto no construtor.

- Comunicar à **CERT.br / NIC.br** (cert@cert.br) e à **SaferNet** (denuncie@safernet.org.br), bem como ao departamento de marca e segurança da **Claro S.A.**
- Monitorar variações do mesmo padrão de nome (claro-faturas.*, claro-pagamento.*, claro-fatura.*, central-claro.*, etc.) pela possibilidade de pertencerem à mesma operação ou serem o próximo destino do operador após takedown.

Anexo A — Manifesto de Integridade das Evidências

Os arquivos abaixo foram preservados na subpasta `evidencias/` (ou `imagens/` conforme indicado) e seus resumos criptográficos (SHA-256) foram calculados ao final da coleta. Qualquer alteração posterior de um arquivo modificará seu hash, permitindo a detecção. O manifesto também está salvo em texto em `evidencias/hash_manifest.txt`.

Arquivo	SHA-256
evidencias/rdap_raw.json	084556c396b615368833372bbf64dcc3fd84edda27d27b03be0331fe3b7ef856
evidencias/rdap_claro-faturas.com.json	6a05d88d5ad7e9ccfe8f8e9c7412473861125957070 3be8dcd139ad84cb26dec
evidencias/dns_claro-faturas.lat.txt	51ee99e580483781a13865a2d06da2d18892cce192647f3faf47dc6b76b51a52
evidencias/headers_https.txt	289794c17e0e824491f0436847e5833e6412992479ec81e0ebd2a6fafc4586d2
evidencias/corpo_https.html	48159ea20fdce29823a79b634a956f45185bcba651d1dc9ce275eb48df312897
evidencias/headers_http.txt	0d51704ee4c1bb548f733fe2a827fac51f2ff205a5ee37ecbfc8e757dd598929
evidencias/corpo_http.html	ec6a0587a0c97bd585f703d24a530d50e26d8ad580ea995d253b79840884ac73
evidencias/ssl_cert.txt	2b614801f3a7e9477954ff6e9e84ef69469814573a14de2a6f90b8f73f0d3536
evidencias/ipinfo.json	f3de4534eb304f6b11755d5092960c41b83eb6bcf64b805dc41d0f172d6870b3
evidencias/ipapi.json	14a44e31a66cde448030cda3662b85acf5a0093e7a688014299b347791d282e7
evidencias/ip_geolocalizacao.txt	5210b31c423b23fd66ce777a2964be5b1343572ba987ca2a221a2426ba9443b6
evidencias/urlscan_search.json	47c1e6a958c1c06b4e5b61f56cbf2f582504026dda272da8d79404938a18cc14
evidencias/urlscan_irmas_dominio.json	9519455331f23dd74f76d5ff27719db19f2809b324ecb79ca00df6daafa82be0
evidencias/urlscan_claro-faturas.com.json	4be43eaad7b15ca1d664dc4848217b0c166b3c4314aaaf3f881a08b842a0dc91
evidencias/wayback_cdx.json	37517e5f3dc66819f61f5a7bb8ace1921282415f10551d2defa5c3eb0985b570
evidencias/corpo_claro-faturas.com.html	356be4014c86b530358f79a318a55f34a0a6ad0c53848b7e77328a6c6f1cdece
evidencias/headers_claro-faturas.com.txt	2cb6ed3497de98ec8b02c5c22054ae7b664c8abb4ec63afd0479a753c84df39a
evidencias/js_claro-faturas.com.js	a9f6ab2670416e3bec369fd0d428b98882d9c89ddb205dcdbb16b41e99dad5a6
evidencias/curl_public_resolver.log	476896691835d47edce768f5954bd23b9ab92398996a24bd8e735fac49b597ec
imagens/urlscan_screenshot_2026-03-23.png	2e29d916e8c80b3f1f2672cdce15d33c4c9488d283fd7c6df0cdba78360c17b1

imagens/lovable_preview_atual_claro-faturas.com.png	0bb302f6bfd70e3fa606bec8a8e6d7d0220bb35d467e4ee050d35b32dd0fb73f

Coleta realizada em 26/05/2026 entre 03:49 e 04:00 UTC. Algoritmo de verificação: SHA-256. Comando de verificação sugerido (a partir da pasta do laudo): `sha256sum -c evidencias/hash_manifest.txt`. A captura de tela na Figura 1 (*urlscan_screenshot_2026-03-23.png*) é, por sua origem, um **arquivo público de terceiros** (urlscan.io) preservado em 23/03/2026 — sua autenticidade pode ser independentemente verificada acessando `https://urlscan.io/result/019d1ae4-6d13-7117-b908-a55c455e3e2a/`.

— Fim do relatório —

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