RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, forense e de risco de fraude do domínio

sephora-mundo.shop

Objeto investigado	sephora-mundo.shop — uso indevido aparente da marca **Sephora**
Natureza	Verificação de legitimidade / suspeita de fraude (typosquatting de marca de cosméticos)
Estado do alvo	Domínio SUSPENSO pelo registrar (status EPP "client hold"). DNS não resolve; sem servidor web ativo.
Data da coleta	21/05/2026 — 04:25 a 04:50 UTC (01:25–01:50 BRT)
Métodos	OSINT passivo · RDAP (GMO Registry + Hostinger) · DNS autoritativo · Certificate Transparency (crt.sh) · Wayback / archive.today / urlscan.io
Emissão do laudo	21/05/2026 às 01:57

1. Sumário Executivo

Este relatório documenta a investigação técnica do domínio **sephora-mundo.shop**, cuja construção léxica ("sephora" + sufixo "-mundo") sugere **typosquatting** da marca de cosméticos **Sephora** — operada no Brasil pelo domínio oficial sephora.com.br (do Grupo LVMH). A coleta foi realizada em 21/05/2026 por meio de técnicas de OSINT (inteligência de fontes abertas) e análise forense passiva.

Na data desta coleta, o domínio **não resolve em DNS** (NXDOMAIN no registro autoritativo do TLD .shop) e seus servidores de nome registrados são `ns1/ns2.dns-parking.com` — plataforma de "parking" da Hostinger usada quando um domínio é colocado **fora do ar de forma forçada**. O registro do TLD informa o status EPP **"client hold"**, indicando que o próprio registrar (Hostinger) suspendeu o domínio — providência típica em resposta a denúncia de abuso/phishing/falsificação de marca.

Cruzando os registros do RDAP do TLD com os logs públicos de Transparência de Certificados (*Certificate Transparency*), é possível reconstruir o ciclo de vida da operação: o domínio foi **registrado em 17/02/2026**, obteve quase imediatamente um certificado Let's Encrypt (emitido na mesma data, com validade de 90 dias) e teve sua última alteração de estado em **27/03/2026** — compatível com a aplicação do "client hold". A vida útil operacional estimada é de aproximadamente **5 a 6 semanas**. Nenhum serviço público de arquivamento (Wayback Machine, archive.today, urlscan.io) preservou conteúdo do site, indicando que ele desapareceu antes de ser indexado.

CLASSIFICAÇÃO DE RISCO	ALTO RISCO DE FRAUDE · domínio já suspenso

A classificação considera (i) o evidente padrão de typosquatting de marca conhecida, (ii) a curta vida útil do domínio e (iii) a ação corretiva já adotada pelo registrar. O fato de o domínio **já estar suspenso** é, por si só, uma confirmação retroativa de risco: o registrar (Hostinger) só aplica "client hold" mediante violação de Termos de Uso ou denúncia formal de abuso. Quem porventura tenha efetuado pagamentos a este endereço entre 17/02 e ~27/03/2026 deve adotar as medidas reativas descritas na Seção 11 (recomendações).

2. Metodologia e Cadeia de Custódia

A investigação seguiu o princípio da **preservação probatória**: todas as respostas de rede foram salvas em arquivo no momento da coleta e tiveram seu valor de resumo criptográfico (hash SHA-256) calculado, permitindo a verificação de integridade a qualquer tempo. Nenhuma técnica intrusiva foi empregada — apenas requisições equivalentes às de um visitante comum e consultas a bases públicas (RDAP, DNS, registros de Certificate Transparency e serviços de arquivamento). Como o servidor web está inacessível, as etapas habituais de coleta de HTTP/TLS/imagens/JS não foram aplicáveis, e essa limitação é registrada no laudo.

Etapa	Técnica / fonte	Evidência preservada
Registro no TLD	RDAP — GMO Registry (operador do .shop)	`rdap_raw.json`
Registro no registrar	RDAP — Hostinger	`rdap_hostinger.json`
Bootstrap de RDAP	IANA RDAP (consulta do servidor para o TLD)	`rdap_iana.json`
Resolução DNS	dig com resolvers públicos (1.1.1.1, 8.8.8.8) e autoritativos (a.gmoregistry.net)	`dns.txt`
Certificate Transparency	crt.sh (registro público de emissão de certificados X.509)	`crtsh.json`
Snapshots históricos	Internet Archive (Wayback) — CDX e Available APIs	`wayback_cdx.json`, `wayback_available.json`

Arquivamento alternativo	archive.today (archive.ph)	`archive_today.html`
Capturas de scanner	urlscan.io (busca por domínio)	`urlscan_search.json`
HTTP / TLS / imagens / JS	Tentativa de coleta — não aplicável (domínio não resolve)	`coleta_resumo.txt; headers_https.txt (vazio, registro de tentativa)`

Todos os artefatos estão na pasta **evidencias/** e seus hashes constam do Anexo A. Fuso de referência: UTC; conversões para 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 **.shop** (GMO Registry — Japão) e complementados pelo RDAP do registrar (Hostinger operations, UAB — Lituânia). O TLD .shop não exige verificação de identidade do titular; ambos os RDAP retornam os dados pessoais **redigidos por privacidade**, deixando visível apenas o país do registrante.

Domínio	sephora-mundo.shop
Handle do domínio (GMO)	DO16585071-GMO
Data de registro	17/02/2026 07:34:56 UTC — **~3 meses na data da coleta**
Data de expiração	17/02/2027 — período mínimo (1 ano)
Última alteração (GMO Registry)	27/03/2026 04:09:44 UTC — **provavelmente a aplicação do client hold**
Status EPP	**client hold** · **client transfer prohibited** · add period
Significado de "client hold"	Suspensão imposta pelo próprio **registrar** — domínio retirado da zona DNS pelo Hostinger; serviço web fica inalcançável.
Servidores de nome registrados	ns1.dns-parking.com · ns2.dns-parking.com (parking da Hostinger)
Registrar (registro junto ao TLD)	**HOSTINGER operations, UAB** — IANA Registrar ID 1636 (Lituânia)
Contato de abuso do registrar	abuse@hostinger.com · +1-212-252-2172
Titular (Registrant)	Redigido por privacidade (Privacy Protection Provided by Hostinger) — país declarado: LT (Lituânia)
DNSSEC	Não assinado (delegationSigned: false)
Operador do TLD .shop	GMO Registry, Inc. (Tóquio, Japão) · RDAP: rdap.gmoregistry.net

Leitura técnica. O domínio foi registrado há ~3 meses, com prazo mínimo (1 ano), em um TLD historicamente associado a alto índice de abuso (.shop). O titular optou pela proteção de privacidade oferecida pela Hostinger, o que é legal mas elimina qualquer responsabilização direta a partir do RDAP. O dado decisivo é o estado EPP **"client hold"**: trata-se de uma medida disciplinar imposta pelo registrar, geralmente em resposta a denúncia de abuso (phishing, violação de marca, fraude). Após o client hold, o domínio é redirecionado para os NS de parking (`dns-parking.com`) e retirado da zona pública.

4. Infraestrutura de DNS

Consultas DNS realizadas tanto via resolvers recursivos (Cloudflare 1.1.1.1, Google 8.8.8.8) quanto diretamente ao servidor autoritativo do TLD (`a.gmoregistry.net`) retornaram **NXDOMAIN** — o domínio simplesmente não existe na zona DNS pública. O resumo:

Registro	Valor	Observação
A / AAAA	— (NXDOMAIN)	Sem registro de endereço — site inalcançável por DNS.
NS (declarados no TLD)	ns1.dns-parking.com · ns2.dns-parking.com	Servidores de "parking" da Hostinger; ativos apenas para apresentar página de "domínio suspenso".
MX	— (NXDOMAIN)	Sem MX — domínio não recebe e-mail.
TXT / SPF	— (NXDOMAIN)	Sem políticas de e-mail nem tokens de verificação.

SOA (autoritativo .shop)	`a.gmoregistry.net · noc.gmoregistry.net · serial 1779337926`	Resposta da zona `shop.` ao consultar o subdomínio.
Status da consulta	`opcode: QUERY, status: NXDOMAIN; flags: qr aa rd`	Resposta autoritativa e definitiva: o domínio não existe na zona.

Foram testados ainda subdomínios comuns em fraudes de e-commerce (`www, admin, login, pagamento, checkout, pay, api, cdn, cliente, conta, order, pedido`): **todos retornaram NXDOMAIN**, confirmando a desativação completa do domínio na zona pública.

Leitura técnica. O conjunto NXDOMAIN + NS de parking + status "client hold" é a assinatura inequívoca de um domínio derrubado pelo registrar. Antes do client hold, ele certamente apontava para algum IP de hospedagem (provavelmente da própria Hostinger, prática típica do registrar/hosting integrado), mas essa informação não está mais disponível em fontes públicas.

5. Hospedagem e Geolocalização do Servidor

Não há atualmente **servidor web acessível** associado ao domínio: a ausência de registro A na zona impede a identificação do IP de hospedagem em uso pela operação fraudulenta. Os únicos endereços pertinentes são os dos servidores de "parking" do registrar — irrelevantes para a análise forense da operação, pois não hospedaram o conteúdo do site.

IP do servidor de origem	**Não disponível** — domínio retirado da zona DNS após o client hold
Registrar / hosting provável (inferência)	**Hostinger operations, UAB** — registrador é também provedor de hospedagem; é prática comum o cliente da Hostinger usar seu hosting integrado.
Servidor web (na época ativa)	Inferido como hospedagem padrão Hostinger (LiteSpeed/Apache + cPanel) — não confirmável post-mortem.
NS atualmente publicados	ns1.dns-parking.com · ns2.dns-parking.com (parking da Hostinger; resolvem para infraestrutura corporativa do registrar — sem relevância forense).

Postura quanto a provedores de infraestrutura. A Hostinger é um provedor de hospedagem/registro de domínios estabelecido (sediada na Lituânia, com operação global), amplamente utilizado por clientes legítimos. O fato de a operação fraudulenta ter sido contratada nesse provedor não imputa, isoladamente, conduta ilícita à empresa — pelo contrário, o registrar agiu, suspendendo o domínio. O ponto registrado neste laudo é o factual: o domínio foi contratado lá e foi lá derrubado.

6. Certificado TLS / HTTPS (via Certificate Transparency)

Não é possível realizar handshake TLS direto com o servidor (item 5). Foi consultado o registro público de Certificate Transparency em `crt.sh`, que preserva permanentemente os certificados X.509 emitidos por autoridades certificadoras participantes — incluindo Let's Encrypt. A consulta retornou um único certificado já emitido para o domínio:

Titular (Subject)	CN = sephora-mundo.shop
Emissor (Issuer)	Let's Encrypt — autoridade "R12" (C=US)
Tipo de validação	DV — Domain Validation (validação apenas de domínio, gratuito)
Válido de	17/02/2026 06:59:42 UTC
Válido até	18/05/2026 06:59:41 UTC — **já expirado**
Número de série	0571651097f554bf72ce00ccd39150de7dd0
Logs CT (publicação)	17/02/2026 07:58:12 UTC (presença em 2 logs CT independentes)

Leitura técnica. A emissão do certificado **na mesma data do registro do domínio** (diferença de minutos) é compatível com a montagem automática típica de fraudes em escala: o operador compra o domínio na Hostinger, ativa hospedagem integrada com Let's Encrypt automático e publica o site em poucos minutos. Certificados DV gratuitos da Let's Encrypt **não atestam a identidade do estabelecimento** — apenas a posse técnica do domínio. O "cadeado" do navegador, portanto, não dá qualquer garantia de idoneidade comercial.

7. Análise do Conteúdo da Página

Não foi possível examinar o conteúdo do site na data desta investigação: o servidor está inalcançável (Seção 4) e não há nenhuma cópia preservada em serviços públicos de arquivamento. As consultas realizadas:

Serviço	Resultado
Internet Archive — Wayback Machine (CDX api)	Nenhum snapshot capturado para o domínio (resposta: `[]`).
Internet Archive — Available API	`archived_snapshots: {}` — confirma ausência.
archive.today (archive.ph)	Página de consulta retornada sem registros próprios para o domínio.
urlscan.io (público)	`total: 0` — nenhum scan submetido publicamente.

Leitura técnica. Domínios fraudulentos de vida útil curta frequentemente "escapam" dos rastreadores automáticos de arquivamento — Wayback indexa mais agressivamente alvos populares, e archive.today/urlscan dependem de submissão humana. A ausência total de cópias é, portanto, **esperada** para um domínio que existiu por ~5 a 6 semanas e foi divulgado provavelmente por anúncios pagos em redes sociais — um vetor de distribuição que não dispara arquivamento espontâneo.

7.1. Marca aparentemente usurpada

Independente do conteúdo específico que tenha sido servido, a construção do nome `sephora-mundo.shop` indica **typosquatting / cybersquatting de marca**:

Termo	Análise
"sephora"	Marca registrada internacionalmente da rede de cosméticos **Sephora** (grupo LVMH). No Brasil, opera oficialmente sob `sephora.com.br` (HTTP 200 na coleta) — registrado e operado pela própria empresa.
"mundo"	Sufixo genérico em português, comum em pseudonimias de fraude ("mundo da Sephora", "Sephora pelo mundo").
".shop"	TLD genérico amplamente utilizado em fraudes de e-commerce — sem qualquer relação com a marca Sephora, que opera no .com e .com.br oficialmente.

Leitura técnica. Não há registro de licenciamento conhecido da marca Sephora para terceiros operarem em domínios derivados — o uso "sephora-mundo" no nome do domínio configura aparente apropriação indevida de marca, infração comumente denunciada via mecanismos UDRP (ICANN) e que, no caso concreto, parece ter sido tratada extrajudicialmente pelo registrar através do client hold.

8. Análise do Fluxo de Pagamento

A análise do fluxo de pagamento depende da inspeção do código JavaScript e do HTML servido pela aplicação — ambos indisponíveis para este caso (Seções 4 e 7). Por consequência, **não é possível afirmar tecnicamente** qual mecanismo (PIX, cartão, agregador de pagamento) era utilizado pelo operador do site.

Padrões observados em casos similares de typosquatting de marcas de cosméticos hospedados em provedores generalistas (Hostinger, Hostgator, BlueHost), publicamente documentados, costumam envolver um destes dois modelos:

Modelo	Características
PIX direto / agregadores	Checkout finaliza em "copia e cola" PIX ou QR Code com beneficiário diverso do estabelecimento anunciado. Sem mecanismo de estorno (chargeback) e com baixa rastreabilidade ao consumidor.
Cartão via gateway desconhecido	Coleta de dados de cartão em formulário próprio (não em checkout transparente regulado), com risco de captura indevida (skimming / phishing).

Leitura técnica. Esta seção é mantida como **placeholder informativo**. Caso o solicitante disponha de prints da etapa de pagamento ou de comprovantes PIX/cartão associados a este domínio, recomenda-se aditar o laudo conforme o procedimento descrito em `docs/prompt_investigacao.md` (adendo de checkout PIX), com decodificação EMV/BR Code da chave/payload PIX e identificação do recebedor real.

9. Indicadores de Fraude (IoF)

A tabela consolida os indicadores objetivamente identificáveis. Cada indicador é classificado pela sua severidade isolada; a **convergência** sustenta a classificação de risco atribuída ao caso.

#	Indicador	Evidência observada	Severidade
1	Typosquatting / uso indevido de marca	Nome contém "sephora" (marca LVMH); domínio oficial brasileiro é sephora.com.br	ALTA
2	Domínio recém-registrado	Registro em 17/02/2026 (~3 meses na coleta); prazo mínimo de 1 ano	ALTA
3	Domínio suspenso pelo registrar (client hold)	Status EPP "client hold" desde ~27/03/2026	ALTA
4	Registrar/hosting integrado com privacy protection	HOSTINGER operations, UAB (LT); titular redigido por privacidade	MÉDIA
5	TLD .shop	TLD genérico com alta taxa estatística de abuso em e-commerce	MÉDIA
6	NS apontando para serviço de parking	ns1/ns2.dns-parking.com (parking da Hostinger)	ALTA
7	Certificado TLS DV gratuito de curta duração	Let's Encrypt R12 emitido em 17/02/2026, expirado em 18/05/2026	MÉDIA
8	Vida útil operacional muito curta	~5 a 6 semanas entre registro (17/02) e suspensão (~27/03/2026)	ALTA
9	Ausência total de rastros em serviços de arquivamento	Wayback / archive.today / urlscan.io: 0 capturas	MÉDIA
10	Sem MX / SPF / TXT — sem e-mail corporativo	Domínio nunca configurou recebimento de e-mail	BAIXA
11	DNSSEC desativado	delegationSigned: false	BAIXA

Síntese: 5 indicadores de severidade ALTA, 4 de severidade MÉDIA e 2 de severidade BAIXA. A combinação **typosquatting + domínio recente + suspensão pelo próprio registrar** é praticamente conclusiva para o perfil de site fraudulento de curta duração — modelo descartável tipicamente associado a campanhas de anúncios em redes sociais que dirigem usuários a uma falsa loja com preços extremamente vantajosos.

10. Conclusão Técnica

Com base nas evidências coletadas e preservadas em 21/05/2026, conclui-se que o domínio **sephora-mundo.shop** apresenta **alto risco de fraude**. A construção do nome configura aparente uso indevido da marca **Sephora**; o domínio foi registrado em 17/02/2026 e **suspenso pelo próprio registrar (Hostinger) em torno de 27/03/2026**, mediante a aplicação do estado EPP "client hold". A curta vida útil operacional (~5 a 6 semanas), o uso de certificado Let's Encrypt emitido na mesma data do registro, a ausência de qualquer infraestrutura de e-mail e a redação dos dados de titularidade compõem o perfil clássico de site fraudulento descartável — provavelmente operado em paralelo a outros nomes do mesmo tipo.

Como o servidor já estava fora do ar no momento da coleta e não há cópias arquivadas, este laudo não documenta o conteúdo específico que era exibido aos visitantes (catálogo, preços, formulário de pagamento, depoimentos, etc.) — porém a ação corretiva já adotada pelo registrar é, tecnicamente, uma **confirmação retroativa** de que o site violou os Termos de Uso (Hostinger documenta o uso de "client hold" especialmente para casos de phishing, falsificação de marca e atividades fraudulentas).

Ressalva metodológica: este laudo baseia-se exclusivamente em fontes abertas e nos metadados públicos preservados (RDAP, DNS, Certificate Transparency). A classificação expressa um juízo técnico de risco e não substitui decisão de autoridade policial ou judicial.

11. Recomendações

Para quem foi vítima ou potencial vítima (acessou o site antes da suspensão)

- **Não tentar reativar a transação** mesmo se receber novo link "atualizado" pelo mesmo vendedor, por e-mail ou WhatsApp — operadores costumam migrar para um novo domínio descartável.
- Caso tenha sido feito pagamento por **PIX**: acionar imediatamente o banco e solicitar o **Mecanismo Especial de Devolução (MED)**, registrando contestação por fraude. O MED tem prazo decadencial curto (80 dias do pagamento) — agir o quanto antes.
- Caso tenha sido feito pagamento por **cartão de crédito**: contestar a transação junto à operadora (*chargeback*) alegando "produto não recebido / fraude" e bloquear o cartão preventivamente.
- **Registrar Boletim de Ocorrência** (delegacia eletrônica do estado) e reunir todas as evidências (prints do anúncio, prints do site, comprovante de pagamento, conversas de WhatsApp).
- Reclamar no **consumidor.gov.br** indicando o domínio `sephora-mundo.shop` e, se conhecido, o nome do beneficiário PIX. Denunciar o anúncio à plataforma em que foi exibido (Meta/Instagram, Google, TikTok).
- Caso tenha fornecido **dados de cartão** no site, **cancelar o cartão** e gerar um novo; em caso de dados pessoais (nome, CPF, endereço, telefone), considerar monitoramento de uso indevido nos seguintes meses.

Para a Sephora Brasil / titular da marca (informativo)

- A Sephora pode acionar a Hostinger (registrar) pelo canal de abuso `abuse@hostinger.com` solicitando documentação adicional sobre o ciclo de vida do domínio, evidências de uso da marca e dados do cliente que registrou o domínio (mediante ordem judicial, se necessário).
- Em paralelo, pode instaurar procedimento UDRP (Uniform Domain-Name Dispute-Resolution Policy) junto à WIPO ou similar para reivindicação formal do nome de domínio — embora, no caso concreto, o domínio já se encontre suspenso (o que torna o UDRP menos urgente, mas ainda relevante para evitar reativação por outro registrante).
- Monitorar o aparecimento de variantes léxicas no mesmo padrão (sephora-*.shop, sephora-mundo.* em outros TLDs, sephora-promo, sephora-oficial, etc.) por meio de serviços de monitoramento de marca em Certificate Transparency.

Para responsáveis técnicos / takedown

- Reportar abuso ao registrar **Hostinger operations, UAB** (`abuse@hostinger.com`) — providência já adotada por terceiro, dada a existência do client hold; novas denúncias reforçam o registro.
- Comunicar à equipe de resposta a incidentes **CERT.br / NIC.br** e à **Safernet Brasil**.
- Se houver capturas privadas (prints, vídeos, comprovantes) do conteúdo do site antes da suspensão, consolidá-las junto a este laudo e ao boletim de ocorrência — essa é a melhor janela para preservar o conteúdo concreto da fraude, dado que serviços públicos não o arquivaram.

Anexo A — Manifesto de Integridade das Evidências

Os arquivos abaixo foram preservados na pasta `evidencias/` e seus resumos criptográficos (SHA-256) foram calculados no momento da coleta. Qualquer alteração posterior de um arquivo modificará seu hash, permitindo a detecção. O manifesto também está salvo em `evidencias/hash_manifest.txt`.

Arquivo	SHA-256
evidencias/archive_today.html	4b433ecd48ad0995762de96f86b081576a0f74d612098f68f6caf2a88c488ae5
evidencias/coleta_resumo.txt	784128548078faa228f4d753ba5f96ff4d39dba6dde1a7e33c6f455250f74b0c
evidencias/crtsh.json	22d4f5a4cdee2cc66f73e97fbf5df5d8c455818265f24f37f648272543edeb19
evidencias/dns.txt	7dc0129eabaf0e196e628f236a2db501dfc88c9e01ba651d117e53c8423c34c7
evidencias/hash_manifest.txt	6c67d4bd5ac4bf7f4ff5663f4c5e660360699b2769200256d85cb019cbd92e98
evidencias/headers_https.txt	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
evidencias/rdap_hostinger.json	c91fdca84aa029df9b6ba606e5e6ed6c24994beada17c854151d74b7c117af1b
evidencias/rdap_iana.json	e2ed9b9ba28c7fead6618f230bfa35b409d68b477abb22d8c9c172b08b902fee
evidencias/rdap_raw.json	c5a898ec36b244b83ba813e935e942b1c4da454299abc42a9bc3a8f4515025a8
evidencias/urlscan_search.json	8c8fb67275daac4a71c59815242f5b390bd6ec349efe60750e5591a3d2a9fb3d
evidencias/wayback_available.json	35e92d3b4224e4f53f223acddf579fcee859a58adcf64679a202906f70727ae4
evidencias/wayback_cdx.json	37517e5f3dc66819f61f5a7bb8ace1921282415f10551d2defa5c3eb0985b570
evidencias/wayback_cdx_wildcard.json	37517e5f3dc66819f61f5a7bb8ace1921282415f10551d2defa5c3eb0985b570

Coleta principal realizada em 21/05/2026, ~04:25–04:50 UTC. Algoritmo: SHA-256. Comando de verificação sugerido: `sha256sum -c hash_manifest.txt` (a partir do diretório raiz da investigação, após ajustar o cabeçalho do arquivo).

— Fim do relatório —

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