RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, forense e de risco do domínio

meusorcamentos.cfd

Objeto investigado	meusorcamentos.cfd (domínio em gTLD .cfd)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	06/06/2026 (RDAP, DNS, HTTP, TLS, geolocalização, crt.sh, Wayback)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · testes de cloaking · crt.sh
Achado central	Conteúdo CAMUFLADO (cloaking) — engodo em branco a observadores
Emissão do laudo	06/06/2026 às 03:05

1. Sumário Executivo

Este relatório documenta a investigação técnica do domínio **meusorcamentos.cfd**, submetido a análise como sítio potencialmente fraudulento. A coleta foi realizada em **06/06/2026** por meio de técnicas de OSINT (inteligência de fontes abertas) e análise passiva, com requisições equivalentes às de um visitante comum, sem qualquer interação intrusiva, exploração de vulnerabilidade ou engenharia reversa de servidor.

O domínio **está no ar** e responde por HTTPS (Apache, certificado Let's Encrypt válido), mas o seu comportamento é o de um **gateway de conteúdo camuflado ("cloaking")**: a todas as requisições observadas — em qualquer navegador, sistema, com ou sem referência de anúncio (Facebook/Google), inclusive simulando origem brasileira — o servidor entrega **uma página propositalmente vazia** de ~198 bytes, cujo único elemento variável é um **título (<title>) com texto aleatório, diferente a cada acesso**. Esse artifício é uma técnica conhecida de **evasão de detecção**: quebra a identificação por assinatura/semelhança de conteúdo usada por scanners de segurança, enquanto o conteúdo verdadeiro (oferta, captura de dados ou pagamento) é reservado apenas a vítimas que cheguem por um canal específico (p.ex. link de anúncio com token de campanha, ou a partir de um IP móvel/residencial brasileiro real). De um ponto de observação neutro, vê-se somente o **engodo**.

Somam-se a isso outros sinais convergentes: domínio **recém-registrado** (17/04/2026), em **TLD barato e frequentemente abusado (.cfd)**, com **dados de titular ocultos**, hospedado em **VPS nos Estados Unidos (Shock Hosting)** — incompatível com o nome em português — e um **subdomínio efêmero** (`rustore.meusorcamentos.cfd`) que teve certificado emitido logo após o registro e já não responde. O nome sugere tema de "orçamentos" em português, mas a própria página declara idioma inglês (`lang="en"`).

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: a **camuflagem ativa de conteúdo** é, por si só, um forte indicador de intenção de enganar — sites legítimos não randomizam títulos nem escondem o conteúdo de observadores. Embora a coleta passiva **não tenha conseguido capturar o payload final** (justamente por ele estar camuflado), o conjunto técnico é típico de **infraestrutura de golpe/phishing**. Recomenda-se **não acessar a partir de dispositivos pessoais, não fornecer dados e não efetuar pagamentos** (ver Seções 7 a 11).

2. Metodologia e Cadeia de Custódia

A investigação seguiu o princípio da **preservação probatória**: todas as respostas de rede e de bases públicas foram salvas em arquivo no momento da coleta e tiveram seu resumo criptográfico (hash SHA-256) calculado. Empregaram-se exclusivamente **técnicas passivas** — requisições de visitante comum e consultas a bases públicas (RDAP via CentralNic/registro do .cfd, DNS, geolocalização de IP, crt.sh e Wayback Machine).

Condições de coleta. O resolvedor DNS local estava indisponível; usaram-se os resolvedores públicos 1.1.1.1 e 8.8.8.8. O cliente HTTP (curl) apresentou instabilidade ao baixar o corpo das respostas do alvo, embora a conexão TLS e as requisições HEAD funcionassem; por isso o corpo HTTPS e os testes de cloaking foram coletados por requisição HTTP/1.1 bruta sobre TLS via `openssl s_client` (arquivos `probe_*.txt`). Os testes de cloaking consistiram em repetir a mesma requisição variando apenas cabeçalhos legítimos de um visitante (User-Agent, Referer, Accept-Language e X-Forwarded-For), comparando as respostas — procedimento estritamente passivo.

Etapa	Técnica / ferramenta	Evidência preservada
Registro do domínio	RDAP — CentralNic (.cfd)	`rdap_raw.json`

Infraestrutura DNS	Consultas dig (A, AAAA, NS, MX, TXT, SOA, CNAME)	`dns_records.txt`
Cabeçalhos / corpo HTTP	curl (HEAD) e openssl s_client (corpo)	`headers_*.txt · corpo_https.html · raw_response.txt`
Teste de cloaking	Requisições com UA/Referer/XFF/paths variados	`probe_*.txt`
Certificado TLS	openssl s_client / x509	`ssl_cert.txt · ssl_raw.txt`
Geolocalização do IP	ipinfo.io e ip-api.com	`ipinfo_*.json · ipapi_*.json`
Certificados (CT)	Transparência de certificados (crt.sh)	`crtsh.json`
Histórico do site	Internet Archive (Wayback — CDX)	`wayback_cdx.json`

Todos os artefatos estão na subpasta **evidencias/** e seus hashes constam do Anexo A. O fuso de referência é UTC.

3. Identificação do Domínio (RDAP)

O domínio está sob o gTLD **.cfd** (registro operado pela CentralNic/ShortDot). Diferentemente do .br, os dados pessoais do titular são **redigidos por padrão** (privacidade de gTLD), de modo que o RDAP expõe apenas o registrador.

Domínio	meusorcamentos.cfd
Data de registro	**17/04/2026 03:07:24 UTC**
Última alteração	22/04/2026 03:12:10 UTC
Data de expiração	17/04/2027 23:59:59 UTC
Idade do domínio	**~7 semanas** na coleta — domínio recente, registro de 1 ano
Titular / Registrant	**Oculto** (dados redigidos — privacidade de gTLD)
Registrador (Registrar)	Dynadot Inc
Servidores de nome	ns1.dyna-ns.net · ns2.dyna-ns.net (DNS do registrador)
DNSSEC	Não assinado (delegationSigned: false)
Status	client transfer prohibited · server transfer prohibited

Leitura técnica. A combinação **TLD barato e abusado (.cfd)** + **registro recente** (menos de dois meses, validade de apenas um ano) + **titular oculto** é um padrão recorrente em domínios descartáveis usados em campanhas de curta duração. A ocultação do titular é prática lícita e comum em gTLDs, mas, somada aos demais sinais, contribui para o **anonimato operacional** típico de operações fraudulentas. Não se imputa conduta ao registrador (Dynadot), mero intermediário de registro.

4. Infraestrutura de DNS

A zona é servida pelos servidores de nome do próprio registrador (Dynadot, `dyna-ns.net`). O apex resolve para um único endereço IPv4; **não há IPv6, MX ou TXT**, e o subdomínio `www` **não resolve**.

Registro	Valor	Observação
A	`104.225.129.176`	VPS Shock Hosting (EUA) — ver Seção 5
AAAA	`— (ausente)`	Sem IPv6
NS	`ns1 / ns2.dyna-ns.net`	DNS do registrador Dynadot
MX	`— (ausente)`	Sem e-mail próprio configurado
TXT / SPF	`— (ausente)`	Sem política de e-mail
SOA	`ns1.dyna-ns.net (serial 2026051201)`	—
www	`— (não resolve)`	Apenas o apex está publicado

Leitura técnica. A ausência de MX/TXT e de IPv6, com apenas o apex publicado em um único VPS, é consistente com um site de **página única** dedicado a uma campanha, e não com uma operação comercial estruturada (que normalmente possui e-mail corporativo e múltiplos registros).

5. Hospedagem e Geolocalização

O endereço atendido pertence a um **provedor de VPS nos Estados Unidos**, o que é **incompatível** com o nome em português e com um público-alvo brasileiro — sinal clássico de hospedagem deslocada para dificultar rastreio e responsabilização.

Endereço IP	104.225.129.176

Sistema autônomo (ASN)	AS395092 — Shock Hosting LLC
Geolocalização (ipinfo.io)	Jacksonville, Flórida — EUA
Geolocalização (ip-api.com)	Jacksonville, Flórida — EUA (hosting: true, proxy: false)
DNS reverso (PTR)	— (ausente)
Servidor web	Apache/2.4.58 (Ubuntu)

Leitura técnica. Trata-se de VPS de baixo custo em datacenter estrangeiro — perfil frequentemente usado por operações efêmeras. Não se imputa conduta à Shock Hosting, provedora de infraestrutura. O fato relevante é a **incompatibilidade entre a hospedagem (EUA) e o público presumido (Brasil)**, somada à ausência de PTR e de e-mail próprio.

6. Certificado TLS / HTTPS

Titular (Subject)	CN = meusorcamentos.cfd
Emissor (Issuer)	Let's Encrypt — autoridade "E7" (C=US)
Tipo de validação	DV — Domain Validation (apenas controle do domínio)
Válido de	12/05/2026 21:16:04 UTC
Válido até	10/08/2026 21:16:03 UTC
Número de série	0689DBCB37FB6FFD3C2754611B006F7CCFED
Fingerprint SHA-256	CF:96:29:5B:D7:F1:06:5E:70:1B:2C:79:90:09:27:A8: 29:25:47:05:8F:26:D0:88:59:EB:F7:9C:43:E4:62:77

A consulta à **Transparência de Certificados** (crt.sh) revelou 8 emissões, todas Let's Encrypt, iniciadas no dia do registro (17/04/2026): apex, `www` e o subdomínio `rustore.meusorcamentos.cfd` (emitido em 18/04/2026), além de reemissão do apex em 12/05/2026. O subdomínio `rustore` **não resolve mais** na data da coleta — vestígio de um recurso efêmero, montado e retirado logo após o registro.

Leitura técnica. O certificado é válido e a conexão HTTPS é legítima do ponto de vista criptográfico — mas certificados DV gratuitos comprovam apenas o controle do domínio, **não a identidade da empresa**, e são abundantes tanto em sites idôneos quanto em fraudes. O histórico em crt.sh é útil sobretudo como linha do tempo: confirma a montagem recente e a existência do subdomínio efêmero "rustore".

7. Análise do Conteúdo — Conteúdo Camuflado (Cloaking)

A página retornada por HTTPS (porta 443; a porta 80 redireciona com 301 para HTTPS) é um **esqueleto HTML vazio** de ~198 bytes: `<html lang="en">` com `<body></body>` sem qualquer conteúdo, script ou imagem. O único elemento que varia é o `<title>`, preenchido com uma **sequência aleatória diferente a cada requisição**. Os cabeçalhos de resposta forçam não-cacheamento (`Cache-Control: no-store, no-cache`; `Pragma: no-cache`) e a existência de `/index.php` confirma uma **aplicação dinâmica em PHP** por trás.

Para verificar se o servidor entrega conteúdo distinto conforme o visitante (**cloaking**), repetiu-se a requisição variando apenas cabeçalhos legítimos. Em **todos** os casos a resposta foi a mesma página vazia (apenas o título aleatório mudou):

Cenário de visitante simulado	Resposta	Título (<title>)
Desktop (Chrome/Windows)	200 · página vazia	`nQ$HV22uF5FqFVmGHc`
Mobile Android	200 · página vazia	`?jPE6TH[L*@(%m+bU>`
iPhone + Referer Google	200 · página vazia	`5g8?wenGM;4,EjD.5^`
Googlebot	200 · página vazia	`a)JECB6F}x5CLgOHE{`
Mobile + Referer Facebook + fbclid	200 · página vazia	`#XI>gzX*Q8hjZ.jXca`
Origem Brasil (XFF/X-Real-IP) + pt-BR	200 · página vazia	`*};wxprug]A2b<0ake`
2 requisições idênticas seguidas	200 · vazias	`dHO7{95#U... ≠ ca5}Eun...`

Duas requisições **idênticas** produziram títulos diferentes, o que prova que a randomização é feita **no servidor, a cada resposta**. O subdomínio `rustore` (no mesmo IP) devolve a mesma página — o servidor é um **catch-all**. `robots.txt` e `sitemap.xml` retornam 404.

Leitura técnica. O conjunto — corpo vazio uniforme + título aleatório por requisição + anti-cache + app PHP — caracteriza um **gateway de cloaking**. A randomização do título é uma técnica deliberada de **evasão**: impede que ferramentas de segurança

agrupem ou assinem o conteúdo. O payload real tende a ser liberado apenas a alvos que cheguem pelo canal "certo" (link de anúncio com parâmetros de campanha, ou IP móvel/residencial brasileiro genuíno na conexão), enquanto observadores (scanners, pesquisadores, IPs de datacenter) recebem o engodo. **Não foi possível capturar o conteúdo final por meios passivos** — e essa própria ocultação é o achado mais relevante. Não foi observado (por estar camuflado) nenhum dos artifícios visíveis de loja-fantasma (contador, falsa escassez, avaliações); a evasão opera em camada anterior.

8. Fluxo de Pagamento

Não foi possível observar o fluxo de pagamento: o conteúdo está **camuflado** (Seção 7) e a página entregue a observadores é vazia, sem formulários, scripts, endpoints (`.php` de pagamento), gateway ou chave PIX visíveis. Também não foi fornecida, para este caso, captura da tela de pagamento/checkout (pasta `pix/`).

Aspecto	Observação
Conteúdo de pagamento visível	Nenhum — página entregue é vazia (cloaking).
Endpoints .php	Há aplicação PHP (index.php), mas a lógica não é exposta a observadores.
Chave PIX estática	Não observável (conteúdo camuflado).
Captura de pagamento (pix/)	Não fornecida para este caso.

Leitura técnica. A ausência de pagamento **visível** não significa ausência de risco — ao contrário: em gateways de cloaking, a coleta de dados e a cobrança costumam ocorrer no payload reservado às vítimas. **Cautela essencial:** qualquer cobrança via PIX, boleto ou cartão associada a este domínio (por anúncio, link ou mensagem) deve ser tratada com forte desconfiança. Se uma captura de tela de pagamento for fornecida, este laudo poderá ser complementado com a decodificação EMV/BR Code e a checagem do recebedor.

9. Indicadores de Fraude

A tabela consolida os achados objetivos. Predominam indicadores de risco; destaca-se a **camuflagem ativa de conteúdo**, de severidade alta por evidenciar intenção de ocultar.

#	Indicador	Evidência	Severidade
1	Conteúdo camuflado (cloaking) com título aleatório por requisição	`probe_*.txt · corpo_https.html`	ALTA
2	Hospedagem em VPS estrangeiro (EUA) incompatível com nome PT	`ip-api/ipinfo · AS395092`	ALTA
3	Domínio recém-registrado (~7 semanas), validade de 1 ano	`RDAP — 17/04/2026`	MÉDIA
4	TLD barato e frequentemente abusado (.cfd)	`RDAP`	MÉDIA
5	Dados do titular ocultos (privacidade de gTLD)	`RDAP — só registrador`	MÉDIA
6	Subdomínio efêmero "rustore" (cert. emitido e já sem resolução)	`crt.sh · DNS`	MÉDIA
7	Incoerência de idioma: nome PT, página lang="en"	`corpo_https.html`	BAIXA
8	Sem e-mail próprio (MX/TXT) e sem PTR	`DNS · PTR vazio`	BAIXA

Síntese: 2 indicadores de severidade ALTA (cloaking e hospedagem deslocada), 4 de severidade MÉDIA e 2 de severidade BAIXA. **Nenhum fator de legitimidade** foi constatado (sem identificação de empresa, sem e-mail corporativo, sem histórico, sem conteúdo verificável).

10. Conclusão Técnica

Com base nas evidências coletadas e preservadas em 06/06/2026, conclui-se que o domínio **meusorcamentos.cfd** opera como um **gateway de conteúdo camuflado (cloaking)**: está no ar, com HTTPS válido, mas entrega deliberadamente uma **página vazia, com título aleatório a cada acesso**, a todo visitante observável, reservando o conteúdo real a alvos que cheguem por um canal específico. Esse comportamento — uma técnica de **evasão de detecção** — soma-se a um conjunto coerente de sinais de risco: registro recente em TLD barato (.cfd), titular oculto, hospedagem em VPS nos EUA incompatível com o nome em português, subdomínio efêmero e ausência de qualquer fator de legitimidade.

Classifica-se o caso como **RISCO ALTO**. A camuflagem ativa de conteúdo é, isoladamente, um forte indício de **intenção de enganar**, compatível com infraestrutura de **golpe ou phishing**. Registra-se, com transparência, que **a coleta passiva não capturou o payload final** — exatamente porque ele está oculto; a conclusão apoia-se no método de evasão e no conjunto de sinais, não na observação direta de uma cobrança ou de captura de dados.

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 ou judicial. O conteúdo entregue às vítimas pode variar no tempo e conforme o canal de chegada.

11. Recomendações

Para o consumidor / solicitante

- **Não acessar o site a partir de dispositivos pessoais** (especialmente celular com IP brasileiro), pois é justamente esse perfil que pode receber o conteúdo malicioso oculto.
- **Não fornecer dados pessoais, login, documentos ou meios de pagamento**, e **não pagar** qualquer PIX, boleto ou cartão associado a este domínio ou a anúncios que levem a ele.
- Desconfiar de anúncios (Facebook/Instagram/Google) e mensagens (WhatsApp/SMS) que conduzam a `meusorcamentos.cfd` — o cloaking é frequentemente usado para burlar a moderação de plataformas de anúncio.
- Se já houve fornecimento de dados ou pagamento: trocar senhas reutilizadas, acionar o banco (e o **MED**, no caso de PIX), registrar reclamação no **consumidor.gov.br** e Boletim de Ocorrência.

Para mitigação / denúncia

- Reportar o domínio às plataformas de anúncio (caso veiculado) e a serviços de bloqueio/Safe Browsing; comunicar o registrador (Dynadot) e o provedor de hospedagem (Shock Hosting) via canais de abuse, anexando este laudo.
- Monitorar a Transparência de Certificados (crt.sh) e o DNS: a emissão de novos certificados ou o surgimento de novos subdomínios indica reativação/expansão da infraestrutura.
- Se for obtida uma **URL de campanha real** (link de anúncio com parâmetros) ou uma **captura de tela** da oferta/pagamento, encaminhar para complementar a análise e tentar caracterizar o golpe específico.

A ausência de conteúdo visível **não** reduz o risco: trata-se de ocultação deliberada. As cautelas acima visam proteger o consumidor diante de uma infraestrutura tecnicamente compatível com fraude.

Anexo A — Manifesto de Integridade das Evidências

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

Arquivo	SHA-256
rdap_raw.json	11295817d23af2920dbbf2c606ee162114d54de8efc9daf3191e4eb45e46d5e8
dns_records.txt	8a22549c8c6a82e4e6b01cc2b18972e7a63b96e7d2525fd21395571f18c3a5b4
headers_http80.txt	ee4cbfb6868d9ee09456259bf20263c57b1793a58c6496d60553ab1744694bef
headers_https.txt	3daf24eacad6a9418a5a64bad7053ba8e87831c70e36be7e779856fd9c76d607
corpo_https.html	85fe5149d618f31de02b50eac5254c739d1df1d29c279eedeb64e854d7297bb1
raw_response.txt	40825c5fbbc3752d50eaf73e608ad5b64ecb0991ae31f516fef1dbd34d869602
probe_desktop.txt	85fe5149d618f31de02b50eac5254c739d1df1d29c279eedeb64e854d7297bb1
probe_mobile.txt	dc1290be37f4b2a69b9d6cd4557e9b20f5aa3c222176601621aa3202ecc970b2
probe_iphone.txt	338f0f153efe227a5f46d9d03e1073d38dbc98aa5612dae4e8dafc9d6f2b9ee2
probe_googlebot.txt	4a6a13cbec0125d24056c8269e28d859a660067561c269b40675683d264a2173
probe_fbref.txt	e68e61145149e286eae632ada90f5566860e88d8f398fab8e1045aeb9db20b15
probe_xff_br.txt	130d4f690c12a81024c2010a06841ccfa927202c3213cd6356396cd49df83cd2
probe_indexphp.txt	f1b7a36c040fce6f56581064529ddbe55a18447ae962584e786dee8349ae6963
probe_rep1.txt	7c91d9fb2c060a0eae75cd0568670c8413a608baf0b27ecf5199af84edbe25cc
probe_rep2.txt	372175dbb057c376bb770c89c85264402a96d6469902e6aed582d6639f1f0325
probe_robots.txt	bd57b534a0e1e979239b6388376ab0fdddfd6bbf2ad4a97993c8215becedf02c
probe_sitemap.txt	ead1780b634ead0d870aa7f941769a62cf7048dcdfd95b18fc59ffe1bac5a54f
probe_rustore.txt	62655baee31dfb35c66f786a25d8e3d550119c54c2441348c8128d837d7f13b7
ssl_cert.txt	041da53b5c86fcf690637487970e0962553ce217e319a1e561bb3308ee231f83
ssl_raw.txt	75a86743fce7ee2e130fc9bfd6469fb9267b5e72639918736bd7abd58ecec8e8
ipinfo_104.225.129.176.json	6d591f0b04eb285953c5af79afbede9d383b7392483d7a1c8c8ad8cfc4c70c97
ipapi_104.225.129.176.json	92d9be7da368ee5be8cc67c215d159c5272a5d9ad3f06aedb41541a31ac8e99e
ptr_reverse.txt	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
crtsh.json	f92dbd85aca2000c5a6d099081b0d20abc8b26b6c2b6af529fdf07e2340beb58
wayback_cdx.json	37517e5f3dc66819f61f5a7bb8ace1921282415f10551d2defa5c3eb0985b570
coleta_notas.txt	9c688f2d8be915c7d70bac00dd9f361b37677282c602aca5d3705d66321338da

Coleta realizada em 06/06/2026 (RDAP/DNS/HTTP/TLS, testes de cloaking, geolocalização, crt.sh e índice CDX do Wayback Machine). Algoritmo: SHA-256. Verificação: `sha256sum -c hash_manifest.txt` (dentro da pasta evidencias/).

— Fim do relatório —

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