

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

casinorich.life

Objeto investigado	casinorich.life - endereço alternativo (“espelho”) do cassino 1win
Natureza	Verificação de vínculo técnico com a marca 1win e do propósito do domínio
Data da coleta	28/11/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bases públicas, análise do código da página)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do HTML e dos scripts
Achado central	Domínio sem relação com o nome da marca que serve a **mesma aplicação do 1win.com**, no mesmo IP, oculto dos buscadores e com título que muda a cada acesso
Classificação	**RISCO ALTO**
Emissão do laudo	28/11/2026 as 01:04

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **casinorich.life**, realizada em **28/11/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem cadastro, sem compra e sem envio de dados pessoais. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O `casinorich.life` foi registrado em 20/08/2025 (465 dias antes da coleta) no mesmo registrador da 1win (URL Solutions/Pananames) e aponta para o mesmo IP do 1win.com, `194.67.193.1` (AS211072 MFI INVESTMENTS LIMITED (Chipre)). A página entregue é a aplicação da 1win em português: mesmo arquivo principal `main-CEwy7_Gr.js`, mesmo identificador de recursos e as metatags `author="1win"`.

Duas diferenças em relação ao domínio principal mostram o propósito: a página pede para **não ser indexada** (`noindex, nofollow`) e o título recebe um número aleatório que muda a cada requisição (“1win: Cassino Online e Apostas Esportivas - 114455.356…”, depois “… - 8124815.055…”), técnica que dificulta a identificação automática do site por listas de bloqueio.

Enquanto o 1win.com não resolve no provedor local, este endereço resolve normalmente — é um **espelho** que mantém o acesso ao cassino. O domínio não é .bet.br e a 1win não usa domínio .bet.br.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: não é um clone nem uma imitação, e sim a própria aplicação da 1win publicada sob um nome neutro, para contornar o bloqueio do domínio principal.

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; o conteúdo, os cabeçalhos e o bundle JavaScript foram obtidos por requisição HTTPS de visitante comum. Nenhum formulário foi preenchido e nenhum dado pessoal foi enviado. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (rdap.org / registro do gTLD / Registro.br)	`rdap_raw.json · rdap_*.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante comum) e navegador headless; home, páginas legais e scripts	`corpo_*.html · headers_home.txt · bundle*.txt`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`geoip.json`
CNPJ declarado	Validação por módulo 11 · base pública BrasilAPI/Receita	`cnpj_publico_*.json`
Consolidação	Extração de fatos e hashes SHA-256	`hash_manifest.txt`

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

Domínio	casinorich.life
Registro	20/08/2025 · expira 20/08/2027 · **465 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)

Registrador	URL Solutions, Inc. · abuse@pananames.com
Servidores de nome	leia.ns.cloudflare.com · osmar.ns.cloudflare.com
DNS - A	194.67.193.1 · sem MX
Hospedagem	AS211072 MFI INVESTMENTS LIMITED · Limassol/CY · cabeçalho `server: cloudflare`
Certificado TLS	Google Trust Services (WE1) · emitido em 16/10/2026 · válido até 14/01/2027
Aplicação servida	Mesmo `main-CEwy7_Gr.js` e mesmo identificador de recursos do 1win.com
Indexação	
Domínio .bet.br	`casinorich.bet.br` — NXDOMAIN

Leitura: domínio de 465 dias, titular oculto, mesmo registrador e mesmo IP da marca.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Mesma aplicação JavaScript do 1win.com, atrás da Cloudflare, sem canônica própria.

Aspecto	Constatação
Conteúdo	Cassino e apostas 1win em português
Título	Número aleatório diferente a cada acesso
Buscadores	`noindex, nofollow`
Acesso no Brasil	Resolve no provedor local, ao contrário do 1win.com

Leitura: a combinação de nome neutro, ocultação dos buscadores e título aleatório é típica de espelho de operador bloqueado.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Mesma aplicação e mesmo IP do 1win.com sob nome sem relação com a marca	`espelhos_1win.txt`	ALTA
2	Oferta de apostas ao público brasileiro fora de domínio .bet.br	`bet_br_check.txt`	ALTA
3	Título com número aleatório a cada acesso (evasão de detecção)	`espelhos_1win.txt`	MEDIA
4	Página oculta dos buscadores (noindex, nofollow)	`corpo_home_resolve.html`	MEDIA
5	Titular oculto	`rdap_raw.json`	BAIXA

Síntese: cinco indicadores, dois de severidade alta. O espelhamento da 1win é o achado central.

6. Conclusão Técnica e Recomendações

O casinorich.life é um endereço alternativo da 1win, que publica a mesma aplicação de cassino e apostas em português sob outro nome, fora de domínio .bet.br e de forma a escapar de buscadores e listas de bloqueio. Classificação técnica: **RISCO ALTO**.

Recomendações ao consumidor / solicitante

- Não deposite em endereços alternativos (“espelhos”) de uma casa de apostas: eles existem justamente para manter o acesso depois que o domínio principal é bloqueado no Brasil.
- No Brasil, só operam legalmente as casas de apostas autorizadas pelo Ministério da Fazenda, sob domínio `.bet.br`; consulte a lista oficial da SPA/MF antes de depositar.
- Não instale aplicativos (APK) baixados fora das lojas oficiais nem informe CPF e dados bancários a operadores sem identificação verificável.
- Em disputa com operador fora do regime autorizado, o apostador não conta com a proteção da regulamentação brasileira para reaver saldo ou saques.

Recomendações de mitigação / denúncia

- Reportar o endereço ao Google Safe Browsing e ao canal de abuso do registrador (abuse@pananames.com).
- Comunicar à Secretaria de Prêmios e Apostas (SPA/MF) e à Anatel a oferta de apostas ao público brasileiro fora do regime autorizado.
- Vítimas que pagaram via Pix: acionar o banco imediatamente pedindo o MED (Mecanismo Especial de Devolução), registrar boletim de ocorrência e reclamação em consumidor.gov.br / Procon, anexando este

laudo.

Ressalva: este laudo expressa **juízo técnico de risco** com base em evidências públicas coletadas passivamente em 28/11/2026; não é decisão judicial e não imputa crime a nenhuma pessoa física ou jurídica. Registradores, provedores de hospedagem/CDN, plataformas de loja e intermediários de pagamento são citados apenas como fatos técnicos, sem imputação de conduta. O titular do site pode usar estes achados para corrigir as inconsistências apontadas. Os fatos podem mudar após a coleta.

Anexo A - Manifesto de Integridade (SHA-256)

Hashes SHA-256 das evidências preservadas no momento da coleta (cadeia de custódia).

Arquivo	SHA-256
bet_br_check.txt (216 bytes)	6846c723e4ffc3eee6aac63df812a0853c58aab165aaaa55a3dcca1fa9b886ba
bundle_js.txt (174858 bytes)	2f5a1caca09886a11682a7a08b06eff2f753d5a2fbb3f2a806c5d48d893685be
corpo_contato.html (106084 bytes)	cd79c9ebd70b8447ae485f3e0965ca27eef00ab5d4bf40f66cb675a18248c121
corpo_faq.html (106083 bytes)	c15bcb598f3217cafd30560c9b609ebfd699b7a83b250b4705c8271bc7019a73
corpo_home.html (105952 bytes)	4668c9dff3ba649ae5c133f9ee7afefbec96a8509bf3701135964cfa2c758660
corpo_home_resolve.html (105801 bytes)	c6e296a0cd4eb47606926641f7755cd15e9b097c762a963c55c9b12949ef1d89
corpo_politica_de_privacidade.html (106083 bytes)	b9315ce95012173d2904aafe07b395fbc1240135bedea3a221de05ca1b7e0a72
corpo_privacidade.html (106085 bytes)	bdab87a4da6026fef072bf395bef0ac047eba2024d0b2a03b37ddf8fe306a54b
corpo_quem_somos.html (106084 bytes)	bb733361f46b3a546782b9114e8d645799f742bab131e642f7b08c6f10ab3744
corpo_sobre.html (106084 bytes)	c565e97888e8ef2bdfa4d7fd8739244b7a03c555e64d0c0320d1edfd36b94537
corpo_suporte.html (106085 bytes)	afcf9fb1afdc5ef6914ce624f188317b814e966127c4eade00397bdd2afde09d
corpo_termos.html (106234 bytes)	63f4ff165e933fa141e7e13f6180eab7e1bd15518621da676bd71cd4c060b2de
corpo_termos_de_uso.html (106085 bytes)	4c0064b42dff2be119258ee2c9b8d9fdc3889e58b79e61c635f71b75becd15b1
dns_records.txt (318 bytes)	3c27ca68e0f852a0640218d6e96d595564b021cf28b2af96cd99db80f74c411b
espelhos_1win.txt (1379 bytes)	1dc02e8778ef1cc3ea9b09bff1b163b31b81bbf64bb2261ca34e94f90a332966
geoip.json (278 bytes)	9b1322826b1ddb9ad8d909d6ca8cb968c179f3b84ebffad0772ab4fdc4f29b8b
headers_home.txt (3228 bytes)	b4c9e1194217e1e6930c9f292ec4f29a917adae82c46febeddd7bdac66982575
headers_home_resolve.txt (3099 bytes)	94ae86f618e01f5f0df02a42566f68bb2518c1220253d120da7552eb416e44ed
rdap_raw.json (7601 bytes)	855f8c4865085896a0a32a836ac9ed0a1d66b1a2130e542e66a6fae8e210b40d
resolvedores.txt (176 bytes)	3f4645923cf3d1c1644125feefc159ae71bec7a53756e31c3c445124eb6acd27
tls_cert.txt (304 bytes)	0bf9239a99e1a3731a4a15818f53459fa397a5913186f8c41a3b6f392e5df693

- Fim do relatório -