

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

1win.com

Objeto investigado	1win.com - domínio principal da marca de cassino e apostas 1win
Natureza	Verificação do regime de operação no Brasil e da infraestrutura da marca
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	Cassino e casa de apostas com versão em português do Brasil (`/pt`) servida fora de domínio **.bet.br**; o domínio não resolve no provedor local, padrão compatível com bloqueio
Classificação	**RISCO ALTO**
Emissão do laudo	28/11/2026 as 01:05

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **1win.com**, 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 1win.com é o domínio principal da marca 1win: registrado em 2002, atrás da Cloudflare, com IP no sistema autônomo AS211072 MFI INVESTMENTS LIMITED (Chipre). A página redireciona o visitante brasileiro para `/pt`, cuja canônica e `hreflang` declaram o público `pt-BR`; o FAQ afirma que a empresa "opera sob uma licença internacional".

No Brasil, a oferta de apostas de quota fixa só é legal para operadores autorizados pela Secretaria de Prêmios e Apostas (SPA/MF), que operam em domínio `.bet.br`. O endereço analisado não é .bet.br e `1win.bet.br` não existe. O provedor de internet local responde **NXDOMAIN** (domínio inexistente) para `1win.com`, enquanto os resolvedores públicos 1.1.1.1 e 8.8.8.8 devolvem o IP normalmente e o mesmo resolvedor local resolve `google.com` — padrão compatível com bloqueio por ordem da Anatel.

A mesma aplicação (mesmo arquivo `main-CEwy7_Gr.js` e mesmo identificador de recursos) está publicada em domínios alternativos no mesmo IP — `casinorich.life`, `wildstake.life` e `1wtedh.com`, analisados em laudos próprios —, que continuam acessíveis no provedor local.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: a marca dirige conteúdo ao público brasileiro sem domínio .bet.br, e o domínio principal já não resolve no provedor local; os espelhos mantêm o acesso aberto.

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	1win.com

Registro	04/07/2002 · expira 04/07/2034 · **8913 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)
Registrador	URL Solutions, Inc. · abuse@pananames.com
Servidores de nome	pranab.ns.cloudflare.com · robin.ns.cloudflare.com
DNS - A	194.67.193.1 · MX: smtp.google.com
Hospedagem	AS211072 MFI INVESTMENTS LIMITED · Limassol/CY
Domínio .bet.br	`1win.bet.br` — **NXDOMAIN** (não existe)
Resolvedor local	NXDOMAIN no provedor local; IP normal em 1.1.1.1 e 8.8.8.8
Versão em português	Canônica `https://1win.com/pt` com `hreflang="pt-BR"`

Leitura: domínio antigo (2002) com titular oculto por serviço de privacidade, registrador URL Solutions (Pananames) e IP de uma rede própria registrada em Chipre.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Aplicação JavaScript própria (bundle `/resources/v1/app/assets/`), atrás da Cloudflare, com dezenas de domínios por país declarados em `hreflang` (`1win.gl`, `1win.ci`, `1win.ng`, `1wincolombia.com` etc.).

Aspecto	Constatação
Público-alvo	Versão `/pt` com `hreflang="pt-BR"`
Licença declarada	“Licença internacional”, sem número nem órgão brasileiro
Domínio .bet.br	`1win.bet.br` inexistente
Acesso no Brasil	NXDOMAIN no provedor local; espelhos ativos no mesmo IP

Leitura: a ausência de domínio .bet.br e o bloqueio no resolvedor local indicam operação fora do regime autorizado; os espelhos analisados à parte reforçam esse quadro.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Oferta em português ao público brasileiro fora de domínio .bet.br	`corpo_home_resolve.html`	ALTA
2	Domínio não resolve no provedor local (padrão de bloqueio)	`resolvedores.txt`	ALTA
3	Mesma aplicação publicada em domínios espelho no mesmo IP	`espelhos_1win.txt`	ALTA
4	Licença apenas “internacional”, sem autorização brasileira	`corpo_home_resolve.html`	MEDIA
5	Titular oculto por serviço de privacidade	`rdap_raw.json`	BAIXA

Síntese: cinco indicadores, três de severidade alta — oferta ao Brasil sem .bet.br, bloqueio no provedor local e espelhos ativos.

6. Conclusão Técnica e Recomendações

O 1win.com oferece cassino e apostas em português ao público brasileiro fora do regime de autorização da SPA/MF, e o domínio não resolve no provedor local. Classificação técnica: **RISCO ALTO** para o apostador brasileiro, que não conta com a proteção da regulamentação nacional.

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 (210 bytes)	ea73935e920ce8acc0d6ddf18adaf5943d57c6ac9cfbd98899dbc021156128cb
corpo_home.html (0 bytes)	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
corpo_home_resolve.html (113930 bytes)	05af30879e7dc39dd83053f53f5757368fecb9b01653a7d3b739346730a30ccd
dns_records.txt (460 bytes)	0272354ffce135a1edc0013e08751eb36cba5d089d118966007989d3ebd845f5
espelhos_1win.txt (1379 bytes)	1dc02e8778ef1cc3ea9b09bff1b163b31b81bbf64bb2261ca34e94f90a332966
geoip.json (278 bytes)	9b1322826b1ddb9ad8d909d6ca8cb968c179f3b84ebffad0772ab4fdc4f29b8b
headers_home.txt (0 bytes)	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
headers_home_resolve.txt (5011 bytes)	108b18ef3eaf31fc60dfd6d996e0739a2adbe7f4aee0e2505948e125880a46c3
rdap_raw.json (2544 bytes)	5adea5b7d38e632450b9b65ed64ee854c0a74df309558659760891327c53b6db
resolvedores.txt (462 bytes)	df016381028d010e2246c6a68c2f57b3583849436d3f6ea0c549209e026b2d00
tls_cert.txt (67 bytes)	fd4601dcf3b285b522c6d9ff265c3abdaa04536ae1abbe191f0a02a66956b40a

- Fim do relatório -