

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

wildstake.life

Objeto investigado	wildstake.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 01:05

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **wildstake.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 `wildstake.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	wildstake.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 02/10/2026 · válido até 31/12/2026
Aplicação servida	Mesmo `main-CEwy7_Gr.js` e mesmo identificador de recursos do 1win.com
Indexação	
Domínio .bet.br	`wildstake.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 wildstake.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 (215 bytes)	13c7ca08daf24b9fa6d53a2b1362d8c486df52d39bd1a87e14468c0f52ef65cd
bundle_js.txt (174858 bytes)	2f5a1caca09886a11682a7a08b06eff2f753d5a2fbb3f2a806c5d48d893685be
corpo_contato.html (106084 bytes)	0964bec9a1fdf2c3d751360f8ace33e7c433d2d6aab1683cc04b7cadaac44873
corpo_faq.html (106084 bytes)	43219aa2cf0fab6d1b4f18bb226c6c12ecfb7d8dca83f86865759787ddc59753
corpo_home.html (105802 bytes)	c6fea24f28a2461fc34278ff79ce82fc7ff560092fd7df9bc9cafba4939f85e4
corpo_home_resolve.html (106021 bytes)	cac9ff220961ea1de3bc296a591d1cbc2676eaf78693ccb99550566320128bd3
corpo_politica_de_privacidade.html (106084 bytes)	2cc794da8335cd386f0d3c8488ca5c6afaa8e91fdb56ff39ad298d5e70f9970d
corpo_privacidade.html (106084 bytes)	c3c3ff8ecd3b47158a8c83e5ab5669bf85dd6e1ff4a162e6aab70ceaaa730d7f
corpo_quem_somos.html (106085 bytes)	1a1c55814940506f9bafc1b1654e06c98f8263b6e6970eb907f3e657ea28ddde
corpo_sobre.html (106084 bytes)	6b13240629ddb126f17a34ab9623cce1d1a20b049d15c834f4b5687644af51e7
corpo_suporte.html (106084 bytes)	4032507ace21ddaad8dabb7c8f60be2fe02deb22251028e099545fadbc6bf9ab
corpo_termos.html (106234 bytes)	ecf336af028adbdc059612a9fe8ddfb6a8baf7af3c5f63e58c7fb4ad3856abee
corpo_termos_de_uso.html (108240 bytes)	2456ef3bfa20d69c92b337714c3fce7604e51b7fb4ae13a429e1179018899be8
dns_records.txt (311 bytes)	94f70370aeb55876c4007101d73e164d4a559fc31ad23ad9c48a370d5c7e6f4d
espelhos_1win.txt (1379 bytes)	1dc02e8778ef1cc3ea9b09bff1b163b31b81bbf64bb2261ca34e94f90a332966
geoip.json (278 bytes)	9b1322826b1ddb9ad8d909d6ca8cb968c179f3b84ebffad0772ab4fdc4f29b8b
headers_home.txt (2159 bytes)	0d4325a51774ac505895593de888d5b4f66ada4c69348cfbda04da83631c346c
headers_home_resolve.txt (3221 bytes)	2ae233b3ff5c932f953fa4aa6f7654763f35bddc39ea62e3035c7f1a8d225d67
rdap_raw.json (7592 bytes)	76ec565ddc527cf7cd84ed1d39ecec60d020544fff8cd8865ef58240f6fb7688
resolvedores.txt (176 bytes)	2b3dab03e63dab46fb2af781a3cc05ec0a46411c90d625d7ea17971dfb70ebed
tls_cert.txt (303 bytes)	1d638d14aa6144ee9d56d206c9326b58a4ea59b5bfb7d7fb2aae8c5a17f2e932

- Fim do relatório -