

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

1wtedh.com

Objeto investigado	1wtedh.com - 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 **1wtedh.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 `1wtedh.com` foi registrado em 16/09/2025 (438 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	1wtedh.com
Registro	16/09/2025 · expira 16/09/2027 · **438 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 03/11/2026 · válido até 01/02/2027
Aplicação servida	Mesmo `main-CEwy7_Gr.js` e mesmo identificador de recursos do 1win.com
Indexação	
Domínio .bet.br	`1wtedh.bet.br` — NXDOMAIN

Leitura: domínio de 438 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 1wtedh.com 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 (212 bytes)	cd232a0a48837ca1f92a8a5d06f9bf186f2e779f48e0774ab209775f60970205
bundle_js.txt (174858 bytes)	2f5a1caca09886a11682a7a08b06eff2f753d5a2fbb3f2a806c5d48d893685be
corpo_contato.html (106235 bytes)	a679e01c14afe77052e194fd70aaec8d20a27c65f390ce22b9915c5a05321060
corpo_faq.html (106084 bytes)	42ef6a9606758a2cf62b7235c1afc2493f80e13dbb681cfee469042971108e75
corpo_home.html (107956 bytes)	3667e8c1a0a77e6899d5a496b0fe51ffd37818f334072c91ba88b816d2a74fdb
corpo_home_resolve.html (105908 bytes)	53f1a02a5d344e9010337952fcfb0ec7146915192292374063a831150c45ca5
corpo_politica_de_privacidade.html (106084 bytes)	eb08084bc1613eb27847bbb3374beff765dabe51398cc3185ee9fc0b039ba29c
corpo_privacidade.html (106234 bytes)	bd7aa3cf2a3ace7a1bacb770bd224952fab02658b21e593847cc8d3ff18bd931
corpo_quem_somos.html (106084 bytes)	ebf5c836d5a991586bfe98d6e6d80645b60b1cb33d4a41c21a35dac67fff3e74
corpo_sobre.html (108239 bytes)	064ef37cfa0b7ef5b2a3b4e884dd6fb059c22a38cf563de87b69fffe2344c4aa
corpo_suporte.html (106085 bytes)	b1efa783f4f2c2a1c4a0b8cf3505371f8e1e9e7d9da0d0e28697bc3ab4392cb7
corpo_termos.html (106235 bytes)	e353296e6fbc11f8aa0dba6d05bb5b7abed7d885c707618fd43faad4c4633f32
corpo_termos_de_uso.html (106084 bytes)	caeef2c19839b2b37514b4d07c97b85654324ccd477b9d392b116f7ca5781da1
dns_records.txt (283 bytes)	5dc2f4efea55550fe45d50399fd9e974e9f0891feb70d038f6ccad3c11a89a2d
espelhos_1win.txt (1379 bytes)	1dc02e8778ef1cc3ea9b09bff1b163b31b81bbf64bb2261ca34e94f90a332966
geoip.json (278 bytes)	9b1322826b1ddb9ad8d909d6ca8cb968c179f3b84ebffad0772ab4fdc4f29b8b
headers_home.txt (2283 bytes)	8301962aaa80fe28a033f7fc87a1631a865a53752c76954cecd46e5db7bff9d7
headers_home_resolve.txt (3202 bytes)	7e3b27d2493f8c4c5fee959ffafaac89d690dc04e75d42d66814c0cdfac39d1e
rdap_raw.json (2560 bytes)	e42b2c2c1a817b884feed537c321e2f47cf0c20c552015aa52d188806449c6d1
resolvedores.txt (176 bytes)	d62e59007855167aa938e401485d62f56e5109eef325aa1d8a69ea6ea684f0ba
tls_cert.txt (299 bytes)	dfa089e0cf6b325a578191a8ff4058a30c5af2bfdf0f16902dd40acf873aa599

- Fim do relatório -