

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

sssgame777.com

Objeto investigado	sssgame777.com - página “Links oficiais da SSSGame Brasil”, hub de espelhos de cassino online
Natureza	Verificação de legitimidade regulatória e de identidade do operador
Data da coleta	17/11/2026 (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	Hub em WordPress que distribui **dezesseis domínios-espelho** da casa de apostas SSSGAME, todos com o mesmo código de indicação, fora do domínio `.bet.br` e bloqueado no DNS de provedor brasileiro
Classificação	**RISCO ALTO**
Emissão do laudo	18/11/2026 as 00:54

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **sssgame777.com**, realizada em **17/11/2026** 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).

A página, em WordPress (Elementor) servida em IP da G-Core Labs em Santana de Parnaíba/SP, apresenta “SSSGAME | Links oficiais de registro” e lista dezesseis endereços — sssgame2.com, sssgame11.com, sssgame22.com, sssgame33.com, sssgame111.com … sssgame999.com, sssgame05/07/08/09.com — cada um com o parâmetro `?code=1166357`, além de perfis de Telegram, Facebook e Instagram “sssgamebrasil”.

O primeiro problema é regulatório. Desde a regulamentação das apostas de quota fixa no Brasil, o operador autorizado pelo Ministério da Fazenda opera obrigatoriamente sob domínio `.bet.br`. A consulta ao Registro.br mostra que **sssgame.bet.br** não existe (RDAP 404), e o domínio investigado é um gTLD genérico. Nenhuma página identifica empresa operadora, licença ou CNPJ.

O resolvedor DNS do provedor de acesso brasileiro usado na coleta **não retorna endereço** para o domínio, enquanto os resolvedores públicos 1.1.1.1 e 8.8.8.8 retornam normalmente — comportamento compatível com as ordens de bloqueio de sites de apostas não autorizados expedidas pela Anatel a pedido da SPA/MF (a inclusão em lista oficial não foi verificada). O conteúdo foi obtido fixando o IP público obtido via 1.1.1.1.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: um hub de “links oficiais” que rotaciona espelhos numerados é a forma usual de manter uma operação acessível apesar de bloqueios — cada domínio derrubado é substituído pelo seguinte (Seções 4 e 5).

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	sssgame777.com

Registro	02/02/2025 · expira 02/02/2027 · **653 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)
Registrador	Gname.com Pte. Ltd. · complaint@gname.com
Servidores de nome	cleo.ns.cloudflare.com · coraline.ns.cloudflare.com
DNS - A	5.188.238.133 · MX: mx.zoho.com, mx2.zoho.com
Hospedagem	AS202422 G-Core Labs S.A. · Santana de Parnaíba/BR · PTR/hostname `20231121.br`
Certificado TLS	TrustAsia Technologies (LiteSSL RSA CA 2025) · emitido em 04/10/2026 · válido até 02/01/2027
Domínio .bet.br	**sssgame.bet.br não registrado** (Registro.br, RDAP 404)
Resolução DNS	Provedor de acesso brasileiro: **sem resposta** · 1.1.1.1 e 8.8.8.8: resolvem (dns_comparativo_resolvedores.txt)
E-mail	MX Zoho · verificação MailerLite no TXT (envio de campanhas)

Leitura: domínio de 2025 (Gname, Singapura) com titular oculto, NS Cloudflare, servidor Apache na G-Core Labs (Brasil) e certificado TrustAsia; e-mail Zoho e MailerLite para campanhas.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

WordPress com Elementor (tema Hello), sem área de jogo própria: a página só distribui links com código de indicação para os espelhos onde ocorrem cadastro e depósito.

Aspecto	Constatação
Função	Distribuidor de espelhos (“links oficiais de registro”)
Espelhos listados	16 domínios sssgameNN.com com `?code=1166357`
Canais	t.me/sssgamebrasilX · facebook.com/sssgamebrasil · instagram.com/sssgamebrasil
Operador	Não identificado; sem licença, sem CNPJ

Leitura: o código de indicação único em todos os links indica uma mesma campanha de aquisição de jogadores.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Apostas ao público brasileiro fora do .bet.br; sssgame.bet.br inexistente	`rdap_raw.json`	ALTA
2	Domínio sem resolução no DNS de provedor brasileiro (compatível com bloqueio)	`dns_comparativo_resolvedores.txt`	ALTA
3	Hub de 16 espelhos numerados para contornar bloqueios	`corpo_home.html`	ALTA
4	Operador sem identificação, licença ou CNPJ	`corpo_home.html`	ALTA

Síntese: quatro indicadores, todos de severidade alta.

6. Conclusão Técnica e Recomendações

O sssgame777.com é um distribuidor de espelhos da casa de apostas SSSGAME, que opera fora do regime brasileiro e sem operador identificado. Classificação técnica: **RISCO ALTO** — oferta de apostas ao público brasileiro fora do regime autorizado, por operador não identificado.

Recomendações ao consumidor / solicitante

- 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 (complaint@gname.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 17/11/2026; 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
corpo_home.html (159393 bytes)	cbc36c9b80d5edc2ee9ece875f97b8f3c0cd0ce19e2c86a09b4c9a45f348af41
dns_comparativo_resolvedores.txt (169 bytes)	5c16fabb0bbf4f2becee8949a01e14ff54fa07d0278130f2280c9562c5a3e2fe
dns_records.txt (482 bytes)	78c47e51ad9f34af6ad184ea6a5eafd232428af47aa5cebe7bf1ab4a693fa161
geoip.json (308 bytes)	a27289bad716535635dc17d5efd18156720e72b08c3d9d1d347c3baff66f933a
headers_home.txt (438 bytes)	4d1f15cc2d74e35036f26a350d710d21b391544d63497fb1cf83af49744597ff
rdap_raw.json (2582 bytes)	bd8fda578963d91e7efcab69fc452fa2f0b36b838c711e38c9fd5e220ef8cc4a
tls_cert.txt (336 bytes)	fca7ccdfb2f35c2b071bb8089751aafdf2e2e7072b77c83c60a738e79510b527

- Fim do relatório -