RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

cherrybux.online

Objeto investigado	cherrybux.online - loja que vende "Robux" (moeda virtual do jogo Roblox) por Pix, sob a marca "Cherry Imperium" (gTLD .online)
Natureza	Verificação de legitimidade e de risco ao consumidor
Data da coleta	02/09/2026 (RDAP, DNS, HTTP/TLS, geolocalização, consulta de CNPJ)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · base pública da Receita Federal
Achado central	A loja afirma "atuamos há mais de 2 anos" e exibe CNPJ próprio, mas o domínio tem **10 dias** e o CNPJ declarado pertence a empresa em situação cadastral INAPTA na Receita Federal
Classificação	**RISCO ALTO**
Emissão do laudo	02/09/2026 as 22:14

1. Sumário Executivo

Este laudo documenta a investigação técnica do domínio **cherrybux.online**, realizada em **02/09/2026** 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 envio de dados pessoais e sem qualquer compra ou pagamento. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O domínio **está no ar** e entrega uma loja intitulada **"Cherry Imperium - Robux Barato | Loja Oficial"**, que vende pacotes de **Robux** - a moeda virtual do jogo *Roblox*, cujo público é majoritariamente infantojuvenil - com preços de **R$ 14,90 a R$ 24,90** e a promessa de "entrega automática" e "Pagamento via PIX com entrega imediata". A página exibe contadores de avaliações (148, 82, 117 estrelas cheias) e um selo de "10% OFF na primeira compra".

O achado central é uma **contradição verificável entre o que a loja afirma e o que as bases públicas mostram**. A página declara: *"aqui na Cherry Imperium, fazemos tudo do jeito certo: somos empresa registrada legalmente sob CNPJ: 37.678.546/0001-06 e já atuamos há mais de 2 anos na venda de códigos digitais"*. A consulta à base pública da Receita Federal confirma que esse CNPJ existe e pertence a **BUX GROUP LTDA** (nome fantasia "BUX GROUP"), aberta em **10/07/2020**, em Conceição do Coité/BA, com CNAE de suporte técnico em tecnologia da informação - mas sua situação cadastral é **INAPTA**. Uma empresa inapta é aquela que deixou de cumprir suas obrigações declaratórias perante a Receita; **não é um CNPJ regular para operar comércio**.

A afirmação de tempo de atuação também não se sustenta no registro do domínio. **cherrybux.online** foi registrado em **23/08/2026** - **10 dias** antes da coleta -, com validade de 1 ano e **titular oculto** no RDAP. Uma loja que "atua há mais de 2 anos" sob esse endereço é incompatível com um domínio de 10 dias.

Há ainda uma **tríplice divergência de identidade**: o domínio é `cherrybux.online`, a marca exibida é **Cherry Imperium** e o e-mail de suporte é `suporte@cherryimperium.com` - um **terceiro** domínio, distinto daquele em que o consumidor está comprando. O único canal de atendimento humano oferecido é um convite de **Discord**; não há telefone, endereço físico, nem páginas legais servidas com conteúdo próprio (as rotas de termos e políticas redirecionam sem entregar documento autônomo). O telefone que aparece no conteúdo é a sequência `1000000000`, isto é, um **preenchimento fictício**. Por fim, a revenda de Robux fora dos canais oficiais do Roblox contraria os termos da própria plataforma e expõe o comprador ao **risco adicional de perda da conta**, além do risco de não recebimento.

CLASSIFICAÇÃO DE RISCO	RISCO ALTO

Leitura: uma loja de 10 dias que afirma atuar "há mais de 2 anos", exibe CNPJ de empresa **INAPTA** na Receita, usa três identidades diferentes (domínio, marca e e-mail), tem telefone fictício e cobra por Pix com atendimento apenas por Discord, oferece **risco elevado**. Recomenda-se **não comprar e não fornecer dados da conta Roblox** (Seções 5 e 6).

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 (Radix / .online - registrador Spaceship)	`rdap_raw.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	`dns_records.txt`

Conteúdo / cabeçalhos	curl HTTPS (visitante comum)	`corpo_home.html · headers_home.txt`
CNPJ declarado	Validação módulo 11 + base pública da Receita (BrasilAPI)	`cnpj_publico_37678546000106.json`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`geoip.json`
Consolidação	Extração de fatos e hashes SHA-256	`hash_manifest.txt`

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

Domínio	cherrybux.online (gTLD .online - registro Radix)
Registro	**23/08/2026** · expira 23/08/2027 · alterado em 28/08/2026
Idade na coleta	**10 dias** - domínio recém-criado
Titular	**Oculto** (o RDAP expõe apenas o registrador)
Registrador	Spaceship, Inc. (IANA 3862) · abuse@spaceship.com
Status	clientTransferProhibited
Servidores de nome	launch1.spaceship.net · launch2.spaceship.net
DNS - A	216.198.79.1 · sem AAAA · **sem MX** · **sem TXT**
Hospedagem	AS16509 Amazon.com · entrega pela plataforma **Vercel** (Server: Vercel)
Aplicação	Next.js (rotas `/_next/static/chunks/`)
Certificado TLS	CN=cherrybux.online · emissor Let's Encrypt YR2 (DV) · válido 23/08/2026-21/11/2026
Emissão do TLS	**no mesmo dia** do registro do domínio
E-mail de suporte	`suporte@cherryimperium.com` - **domínio diferente** do da loja
Sem MX no domínio	A loja **não recebe e-mail** no próprio domínio

Leitura técnica. Registro de 10 dias, titular oculto, validade de 1 ano e ausência de MX (nenhum e-mail no próprio domínio) compõem um perfil de **baixa rastreabilidade do responsável**. O certificado DV gratuito comprova apenas o controle do domínio, **não a identidade de qualquer entidade**. O uso de e-mail em um terceiro domínio (`cherryimperium.com`) e a publicação em plataforma de desenvolvimento (Vercel) são compatíveis com uma operação de **montagem rápida e baixo custo de descarte**. Não se imputa conduta ao registrador (Spaceship), à Amazon nem à Vercel, meros provedores de infraestrutura.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

O site é uma **loja de moeda virtual** construída em Next.js e publicada na Vercel. O catálogo oferece pacotes de Robux (700, 1.200, 1.700, 2.100 e superiores) com preço em reais, selo de desconto na primeira compra e um marcador "ESGOTADO" em um dos itens. O checkout e as rotas de políticas respondem por redirecionamento, sem servir documento legal autônomo ao visitante. O atendimento é dirigido a um convite de Discord.

Afirmação da loja	O que a evidência mostra
"somos empresa registrada legalmente sob CNPJ: 37.678.546/0001-06"	CNPJ existe e é válido, mas pertence a **BUX GROUP LTDA** em situação **INAPTA** na Receita Federal
"já atuamos há mais de 2 anos"	Domínio registrado em **23/08/2026** - **10 dias** antes da coleta
"Loja Oficial"	Não há qualquer indicação de autorização da Roblox Corporation; a revenda de Robux fora dos canais oficiais contraria os termos da plataforma
"entrega automática" / "entrega imediata"	Não verificável de forma passiva; nenhum mecanismo de garantia ou custódia é apresentado
Contato	E-mail em **outro domínio**, telefone `1000000000` (fictício) e apenas convite de **Discord**
Páginas legais	Rotas de termos, privacidade e reembolso **não entregam documento próprio**

Aspecto	Constatação
Tipo de site	Loja de moeda virtual (Robux / Roblox) voltada ao público brasileiro, com público-alvo majoritariamente infantojuvenil
CNPJ declarado	37.678.546/0001-06 - **BUX GROUP LTDA**, Conceição do Coité/BA, aberta em 10/07/2020, situação **INAPTA**
Tempo de atuação alegado	"mais de 2 anos" × domínio de **10 dias**
Identidades divergentes	Domínio `cherrybux.online` · marca "Cherry Imperium" · e-mail `@cherryimperium.com`
Telefone	`1000000000` - **preenchimento fictício**
Endereço físico	**Ausente**
Atendimento	Convite de **Discord** como único canal humano
Páginas legais	Rotas existem, mas **não entregam documento próprio** (respondem por redirecionamento)
Meio de pagamento	**Pix** com promessa de entrega imediata
Prova social	Contadores de avaliações (148, 82, 117) sem qualquer fonte verificável

Leitura técnica. O que torna este caso grave não é vender Robux, mas a **construção deliberada de credibilidade sobre fatos que a base pública desmente**. Exibir um CNPJ é a principal âncora de confiança de uma loja brasileira; aqui, o CNPJ exibido é real, porém de empresa **inapta**, e o texto que o acompanha ("atuamos há mais de 2 anos") é incompatível com um domínio de 10 dias. Não é possível afirmar, por fontes abertas, se quem opera o site tem qualquer relação com a BUX GROUP LTDA - e é justamente essa **impossibilidade de vinculação** que caracteriza o risco: o consumidor confia em um número que não corresponde à operação que tem diante de si. Some-se o público-alvo infantojuvenil, o pagamento por Pix (irreversível na prática) e o atendimento restrito a Discord, e o cenário de prejuízo sem recurso está completo. A coleta foi passiva: nenhuma compra foi feita e nenhum dado enviado.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	CNPJ declarado pertence a empresa em situação INAPTA na Receita Federal	`cnpj_publico_37678546000106.json`	ALTA
2	Afirmação de "mais de 2 anos" de atuação em domínio registrado 10 dias antes da coleta	`corpo_home.html` · `rdap_raw.json`	ALTA
3	Domínio registrado 10 dias antes, titular oculto, validade de 1 ano	`rdap_raw.json`	ALTA
4	Telefone de contato fictício (sequência 1000000000) e ausência de endereço físico	`corpo_home.html`	ALTA
5	Autodenominação "Loja Oficial" sem qualquer indicação de autorização da Roblox Corporation	`corpo_home.html`	ALTA
6	Três identidades distintas: domínio, marca exibida e domínio do e-mail de suporte	`corpo_home.html` · `rdap_raw.json`	MEDIA
7	Rotas de termos, privacidade e reembolso não entregam documento legal próprio	`corpo_home.html`	MEDIA
8	Atendimento humano restrito a convite de Discord, sem telefone ou canal rastreável	`corpo_home.html`	MEDIA
9	Ausência de MX: a loja não recebe e-mail no próprio domínio	`dns_records.txt`	BAIXA
10	Contadores de avaliações sem fonte verificável; TLS DV emitido no mesmo dia do registro	`corpo_home.html` · `tls_cert.txt`	BAIXA

Síntese: 5 indicadores de severidade ALTA, 3 MEDIA e 2 BAIXA. O único fator que aparentava legitimidade - o CNPJ exibido - **foi desmentido pela consulta à base pública**, que o mostra em situação INAPTA.

6. Conclusão Técnica e Recomendações

Com base nas evidências coletadas e preservadas em **02/09/2026**, conclui-se que **cherrybux.online** apresenta **risco alto ao consumidor**. A loja vende moeda virtual do Roblox por Pix a um público majoritariamente infantojuvenil, apresentando-se como "Loja Oficial" e como "empresa registrada legalmente" que "atua há mais de 2 anos". As duas afirmações centrais de credibilidade **não se sustentam nas fontes públicas**: o CNPJ declarado (37.678.546/0001-06) pertence a **BUX GROUP LTDA**, cuja situação cadastral na Receita Federal é **INAPTA**, e o domínio foi registrado **10 dias** antes da coleta. Somam-se a isso o titular oculto, o telefone fictício, a ausência de endereço, o e-mail em domínio diverso, o atendimento apenas por Discord e a inexistência de páginas legais com conteúdo próprio. Classifica-se o caso como **RISCO ALTO**.

Recomendações ao consumidor / solicitante

- **Não comprar e não pagar o Pix**; em caso de dúvida, adquirir Robux apenas pelos **canais oficiais do Roblox** (aplicativo e site oficiais).
- **Jamais fornecer login, senha ou código de verificação da conta Roblox** a terceiros: a entrega de Robux por fora costuma exigir acesso à conta e pode resultar em **perda definitiva da conta** por violação dos termos da plataforma.
- Conferir a situação cadastral de qualquer CNPJ exibido em loja pequena na **consulta pública da Receita Federal**; um CNPJ "INAPTO" ou "BAIXADO" não é apto a operar comércio.
- Comparar o CNPJ e o nome da empresa com o domínio e o e-mail de contato: **três identidades diferentes** num mesmo site é sinal de alerta.
- Se já houve pagamento: acionar o banco e o mecanismo **MED** do Pix, reunir comprovantes e registrar reclamação em **consumidor.gov.br** e Boletim de Ocorrência. Se a compra foi feita por criança ou

adolescente, revisar os controles de pagamento do dispositivo.

Recomendações de mitigação / denúncia

- Denunciar o domínio aos canais de abuse do registrador (`abuse@spaceship.com`) e da plataforma de hospedagem (Vercel), anexando este laudo.
- Comunicar a **Roblox Corporation** o uso da expressão "Loja Oficial" e a revenda de Robux fora dos canais autorizados, para as medidas de proteção de marca cabíveis.
- Se a **BUX GROUP LTDA** não tiver relação com este site, o uso de seu CNPJ deve ser comunicado por ela à Receita Federal e à autoridade policial, por possível apropriação de identidade empresarial.
- Preservar este relatório e as evidências (pasta `evidencias/`, com hashes SHA-256) para eventual uso administrativo ou judicial.

*Ressalva metodológica: este laudo baseia-se em fontes abertas e reflete o estado do domínio na data indicada (coleta em 02/09/2026). A classificação expressa um **juízo técnico de risco** e não substitui decisão de autoridade policial, administrativa ou judicial. **Não se imputa qualquer conduta à BUX GROUP LTDA**, empresa cujo CNPJ aparece exibido no site: não há, nas fontes consultadas, elemento que demonstre vínculo entre essa empresa e este domínio, e ela pode ser vítima do uso indevido de seu registro. Não se imputa conduta ilícita aos provedores de infraestrutura citados (Spaceship, Amazon, Vercel).*

Anexo A - Manifesto de Integridade (SHA-256)

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

Arquivo	SHA-256
`cnpj_publico_37678546000106.json (2142 bytes)`	`bb7a719f84d85c282354a708386ba235f655493c69f0a70384330c72dc0c8bac`
`corpo_home.html (221904 bytes)`	`865d8753e731752eb97197bddbef9937ec0a0aadee1439142052dd2d745892a3`
`dns_records.txt (361 bytes)`	`aab8f73b382f1def2721841226aea5268f9ce65f694f98d0bfffad7910a404c2`
`geoip.json (280 bytes)`	`7e7bc0a546d9f06cdb5d19007f318d02373b355b38ef392434df2ab37340c98b`
`headers_home.txt (1360 bytes)`	`fdaa3e2bea4b5f51eece98fb770e0b11bad790a43db2518e1df12fcd5e537b8f`
`rdap_raw.json (5321 bytes)`	`ec4ad2c515aab85620d1ae89246f488e02a69e9a2574209df87c57b9660c60b5`
`tls_cert.txt (301 bytes)`	`1320191ae15bcb4633bc8ac017072f5c5a5123dadfc97eed1f3aff93c7357f33`

- Fim do relatório -