

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

atacapets.com

Objeto investigado	atacapets.com - loja online que se apresenta como a Atacapet, atacadista de produtos pet de Cariacica/ES
Natureza	Verificação de autenticidade da loja, de vínculo com a empresa declarada e do fluxo de pagamento
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	Domínio de 61 dias, registrado em registrador turco, que reproduz nome, CNPJ e endereço da Atacapet real (dona de **atacapet.com.br** desde 2012) e cujo checkout **grava número, validade e CVV do cartão** após a recusa e empurra o comprador para um Pix com QR codes de um “pool” manual
Classificação	**RISCO ALTO**
Emissão do laudo	18/11/2026 as 00:54

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **atacapets.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).

O site exibe a vitrine de um atacado pet completo — rações Golden e Premier, areia, tapetes, jardim — com "5% de desconto no Pix", frete grátis acima de R$ 199 e o CNPJ **25.096.492/0004-34**, que é de fato uma filial ativa da ATACAPET PRODUCTS COMERCIAL LTDA em Cariacica/ES. O endereço exibido (Av. Mário Gurgel, 5527) também confere com a Receita.

O domínio, porém, não é o da empresa. A Atacapet real usa **atacapet.com.br**, registrado em 2012 no CNPJ-matriz da própria empresa. O endereço investigado — **atacapets.com**, com "s" — foi criado em 17/09/2026 num registrador da Turquia (Atak Domain), com titular oculto; e o canônico que o site declara, **atacapets.com.br**, foi registrado em 04/09/2026 por uma pessoa física sem relação aparente com a empresa.

O achado mais grave está no código do checkout (bundle JavaScript público). Quando o cartão é recusado, a função que chama `/api/save-card` envia ao servidor do próprio site o **número completo do cartão, a validade, o CVV**, o CPF, o endereço e os itens do pedido; em seguida a tela exibe "Oferta única após a recusa do cartão. Pague no Pix e finalize com desconto". O mesmo bundle traz um painel administrativo "**Pool de PIX manual**", no qual o operador cola códigos Pix "copia e cola" de valor fixo, gerados fora do site, e os distribui por faixa de valor de carrinho.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: a identidade da empresa exibida é verdadeira, mas o vínculo dela com o domínio **não é demonstrado** — ao contrário, a empresa possui outro domínio desde 2012. Somado à captura de dados completos de cartão e ao Pix com recebedores definidos fora do site, o conjunto é compatível com **apropriação de identidade** de empresa real (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	atacapets.com
Registro	17/09/2026 · expira 17/09/2027 · **61 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)
Registrador	Atak Domain Bilgi Teknolojileri A.S. · domain@apiname.com
Servidores de nome	maxine.ns.cloudflare.com · pranab.ns.cloudflare.com
DNS - A	104.21.65.163 · 172.67.147.40 · sem MX
Hospedagem	AS13335 Cloudflare, Inc. · San Francisco/US · cabeçalho `server: cloudflare`
Certificado TLS	Let's Encrypt (YE1) · emitido em 15/11/2026 · válido até 13/02/2027
Domínio da empresa real	`atacapet.com.br` · registrado em 19/03/2012 em nome do CNPJ **25.096.492/0001-91** (ATACA PET PRODUCTS COMERCIAL LTDA, matriz)
Domínio vizinho	`atacapets.com.br` · registrado em 04/09/2026 por **pessoa física** (CPF mascarado ***.012.553-**), sem relação aparente com a empresa; é o domínio que o clone declara como canônico
CNPJ exibido	25.096.492/0004-34 · ATACAPET PRODUCTS COMERCIAL LTDA (filial) · ativa desde 14/06/2024 · Cariacica/ES · comércio atacadista de alimentos para animais — dados corretos da empresa real

Leitura: domínio de 61 dias, titular oculto, registrador estrangeiro e um domínio “gêmeo” .com.br em nome de pessoa física, enquanto a empresa real usa atacapet.com.br desde 2012. Hospedagem atrás da Cloudflare, com imagens em CDN Bunny (`atacapet.b-cdn.net`).

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Aplicação React/Vite de página única. O bundle principal (`index-DICBuSLi.js`) e os módulos carregados sob demanda (`CheckoutPage`, `AdminPixPoolPage`) foram baixados como visitante e preservados. A configuração pública do checkout (`/api/checkout-config`) indica cartão via Mercado Pago e o modo padrão `cardGateway: "decline"` quando a configuração falha.

Aspecto	Constatação
Endpoints de API	`/api/create-pix`, `/api/create-card`, `/api/save-card`, `/api/check-payment`, `/api/auth/cpf`, `/api/admin/manual-pix`
Cartão recusado	Envio de `card_number`, `card_expiry`, `card_cvv`, CPF, e-mail, telefone e endereço a `/api/save-card`; depois, tela de “10% OFF só no Pix”
Pix	Painel “Pool de PIX manual”: “Cole o copia-e-cola. O valor (tag 54) e o recebedor são extraídos automaticamente. Só entra QR com valor fixo.” — QRs gerados fora do site, por faixa de carrinho
Dados coletados	Nome, CPF, e-mail, telefone, endereço completo e dados integrais do cartão
Identidade exibida	Nome, CNPJ (filial 0004) e endereço corretos da Atacapet real; telefone (27) 99631-8756

Leitura: armazenar o CVV após a autorização é vedado pelas regras do setor de cartões (PCI-DSS); aqui ele é gravado justamente quando o pagamento falha. E o Pix não é gerado por um intermediário vinculado à loja: o recebedor é quem gerou cada QR colado no pool — **não necessariamente a empresa exibida**.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Domínio de 61 dias, titular oculto, registrador turco — e a empresa real usa outro domínio (atacapet.com.br) desde 2012	`rdap_raw.json · rdap_atacapet.com.br.json`	ALTA
2	Domínio canônico atacapets.com.br registrado em 04/09/2026 por pessoa física sem vínculo aparente	`rdap_atacapets.com.br.json`	ALTA
3	Checkout grava número, validade, CVV e CPF do titular quando o cartão é recusado	`chunk_CheckoutPage-*.txt · bundle_js.txt`	ALTA
4	Após a recusa, oferta “10% OFF só no Pix” — funil de recusa de cartão para Pix	`chunk_CheckoutPage-*.txt`	ALTA
5	“Pool de PIX manual”: QR codes de valor fixo gerados fora do site; recebedor não é a loja demonstrada	`chunk_AdminPixPoolPage-*.txt`	ALTA
6	CNPJ, nome e endereço de empresa real exibidos sem vínculo técnico com o domínio	`cnpj_publico_25096492000434.json`	MEDIA

Síntese: seis indicadores, cinco de severidade alta. O padrão — clone de empresa real em domínio parecido, captura de cartão e Pix com recebedor externo — é típico de loja falsa.

6. Conclusão Técnica e Recomendações

O endereço atacapets.com reproduz a identidade da Atacapet real, mas não pertence a ela: a empresa usa atacapet.com.br desde 2012, e os dois domínios “atacapets” surgiram em setembro de 2026 em nome de terceiros ou com titular oculto. O checkout grava dados completos de cartão (inclusive CVV) quando o pagamento é recusado e direciona o comprador a um Pix cujo recebedor é definido por QR codes colados manualmente. Classificação técnica: **RISCO ALTO**, com indício de apropriação de identidade da empresa — que deve ser tratada como possível vítima, não como responsável.

Recomendações ao consumidor / solicitante

- Para comprar da Atacapet, use o site oficial atacapet.com.br ou o atendimento divulgado pela empresa.
- Quem digitou o cartão em atacapets.com deve pedir o **bloqueio e a troca do cartão** ao banco, mesmo que a compra tenha sido recusada.
- Desconfie de preços muito abaixo do mercado combinados com desconto extra para pagamento via Pix.
- Antes de comprar, confira o CNPJ na Receita Federal e se o domínio do site pertence de fato à empresa (consulta RDAP / Registro.br).
- Prefira cartão de crédito, que permite contestação (chargeback); o Pix é instantâneo e de difícil reversão.

Recomendações de mitigação / denúncia

- Reportar o endereço ao Google Safe Browsing e ao canal de abuso do registrador (domain@apiname.com).
- 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.
- Comunicar a ATACAPET PRODUCTS COMERCIAL LTDA, que pode pedir a suspensão dos domínios por uso indevido de marca.

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
api_checkout_config.json (191 bytes)	adfaf22d74ae7d29b963b3203833539b70f90251c8d364f73a1d9cc9241992bb
bundle_js.txt (381574 bytes)	cfe70c7be5b27ce80f6d0c53aadc5b34c640ecd0d56f490fb8acde8bf4638ec4
chunk_AdminPixPoolPage-FNKkeDG1.js.txt (25780 bytes)	543c09e817d383816ca50fbf3930aab992b7e7c51b2817a6fefe76ddfe2e0bbd
chunk_CheckoutPage-DZbF8ioF.js.txt (52587 bytes)	d31dcf0b6319c347d9fbbffc264e6bafe4950302acb9d010a76466374fefa5ec
cnpj_publico_25096492000434.json (5785 bytes)	8f2e2b34450f418e55b6744e7e6859e8c8a1dd416032c912f0b060ff6e31b2f3
corpo_home.html (147859 bytes)	a5dd0f38fdfb76715b7fc502e63ae9ee35523b9f733af0e9474cf44c250ad59b
dns_records.txt (408 bytes)	0c4ea8dd8e4f703724444c3fed2ec078d15963201d7b7c7c3974ad5f9f987505
geoip.json (288 bytes)	8bdd747ec85950f4633cad1ba43dcf9fa1a447544ba55095a067e3260284bad7
headers_home.txt (1460 bytes)	10b27b0370de9c969dd2fc33f8734c6115f1ac2c45cea7c325c16800d429cccf
rdap_atacapet.com.br.json (3389 bytes)	71d95b41c2a719fb78f0a522e699d3778cf0184eef0eda2fff4b6001cce8e353
rdap_atacapets.com.br.json (4056 bytes)	6808ecddb0787c3ab8fbb9143454150039cb93c99863371fb7b09b24ee85cf0d
rdap_raw.json (2584 bytes)	61e2a19123f654cec5c8224ee1bc2a893109731dbfa8127c2711825cca6fd434
tls_cert.txt (298 bytes)	676c266ad221782d2310edc3cdc771657c379c2efbd1ef9114373f1d1f39931d

- Fim do relatório -