Relatório de OSINT / Pentest — Entrega para Entidade Civil

Realizado por:

Pentester:
Ygor Costa

Pentester:
Natan Fagundes

Data:
10/11/2025

Introdução

Em resumo: investigamos uma campanha de golpes online centrada em páginas de marketplace falsas que oferecem produtos/serviços e capturam pagamentos por PIX. Encontramos domínios ativos que hospedam páginas de pagamento, evidências de comunicação com supostos responsáveis (prints de WhatsApp), e um token JWT ligado a um recurso pix.adyen.com — isso sugere que os golpistas estão usando (ou simulando usar) a infraestrutura de pagamentos da Adyen para criar QR Codes PIX e receber valores.

Para leigos: os criminosos criam sites falsos que parecem lojas. Quando uma vítima tenta pagar, recebe um QR Code/PIX que aponta para um mecanismo (o token JWT) que pode estar vinculado a uma conta real — isso permite rastrear para onde o dinheiro vai se o provedor de pagamento (Adyen) colaborar

Conclusão: alto risco, atuação ativa e possibilidade de rastrear transações via provedores de pagamento e registradores. Recomenda-se ação imediata da entidade civil para preservação de evidências, contato com provedores (Adyen, GoDaddy, UOL, Cloudflare) e notificação de plataformas de anúncios (Google Ads / Meta/Facebook).

Escopo e limitações

- Solicitante: entidade civil (não especificada).

- Objetivo: coleta passiva de evidências públicas (OSINT) para identificar infraestrutura, contas de contato, e indícios de recebimento de valores; produzir relatório para apresentação.

- Ações realizadas: pesquisa passiva (WHOIS/RDAP, inspeção manual das páginas, análise de links, captura de prints, extração de token JWT retornado por recurso HTTP). Nenhuma ação intrusiva ou acessos não autorizados foram realizados.

- Limitação principal: não houve quebra de sigilo judicial nem acesso a logs privados de provedores — recomenda-se solicitar formalmente logs/transações aos provedores identificados.

Dados do alvo

app-mercadodigitalml.com — Marketplace falso (ALVO PRINCIPAL)

Classificação: Golpe / Marketplace falso / Fraude por pagamento (PIX).
URL principal observada: CENSU (página de oferta e formulário de pagamento).

Dados coletados e evidências:

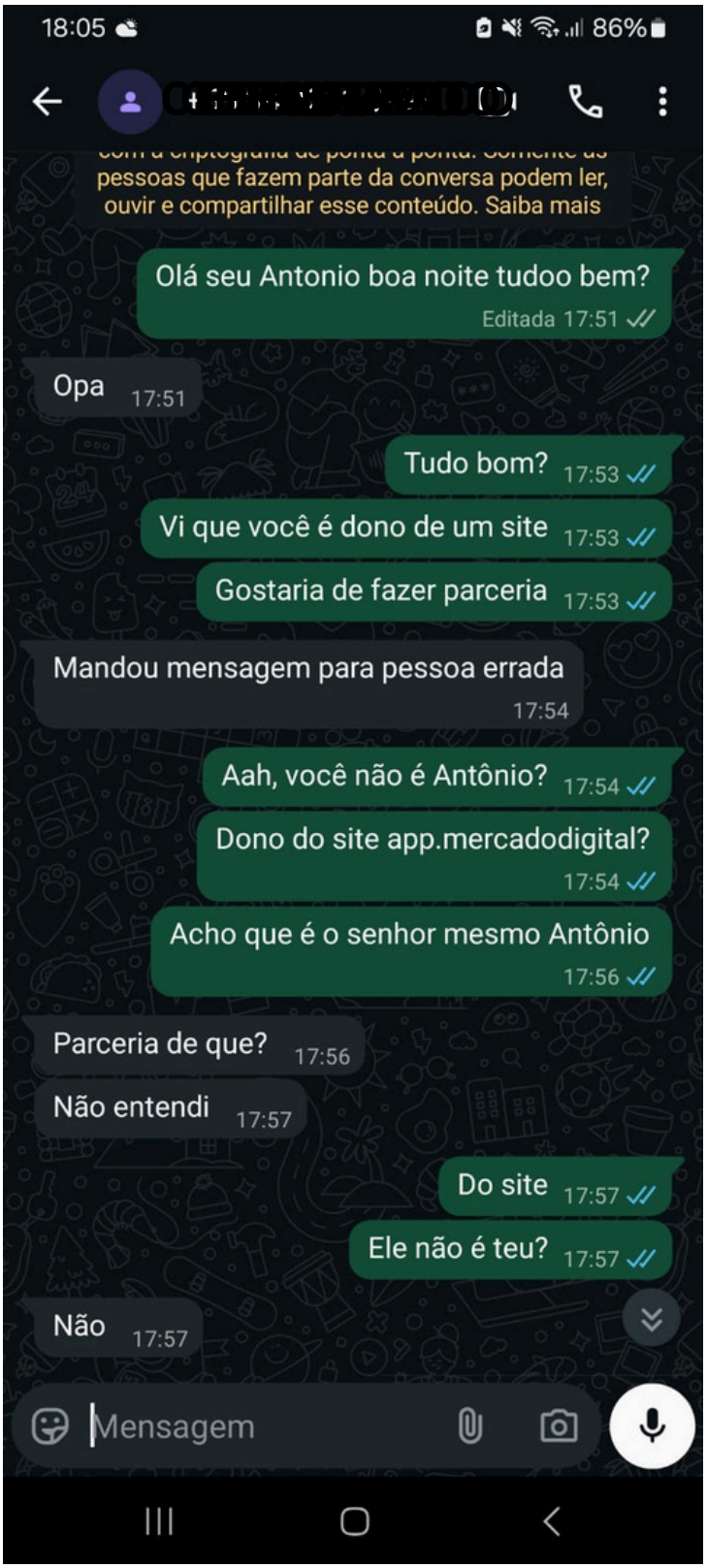
Nome informado em contato: CENSURADO (informação declarada na conversa).

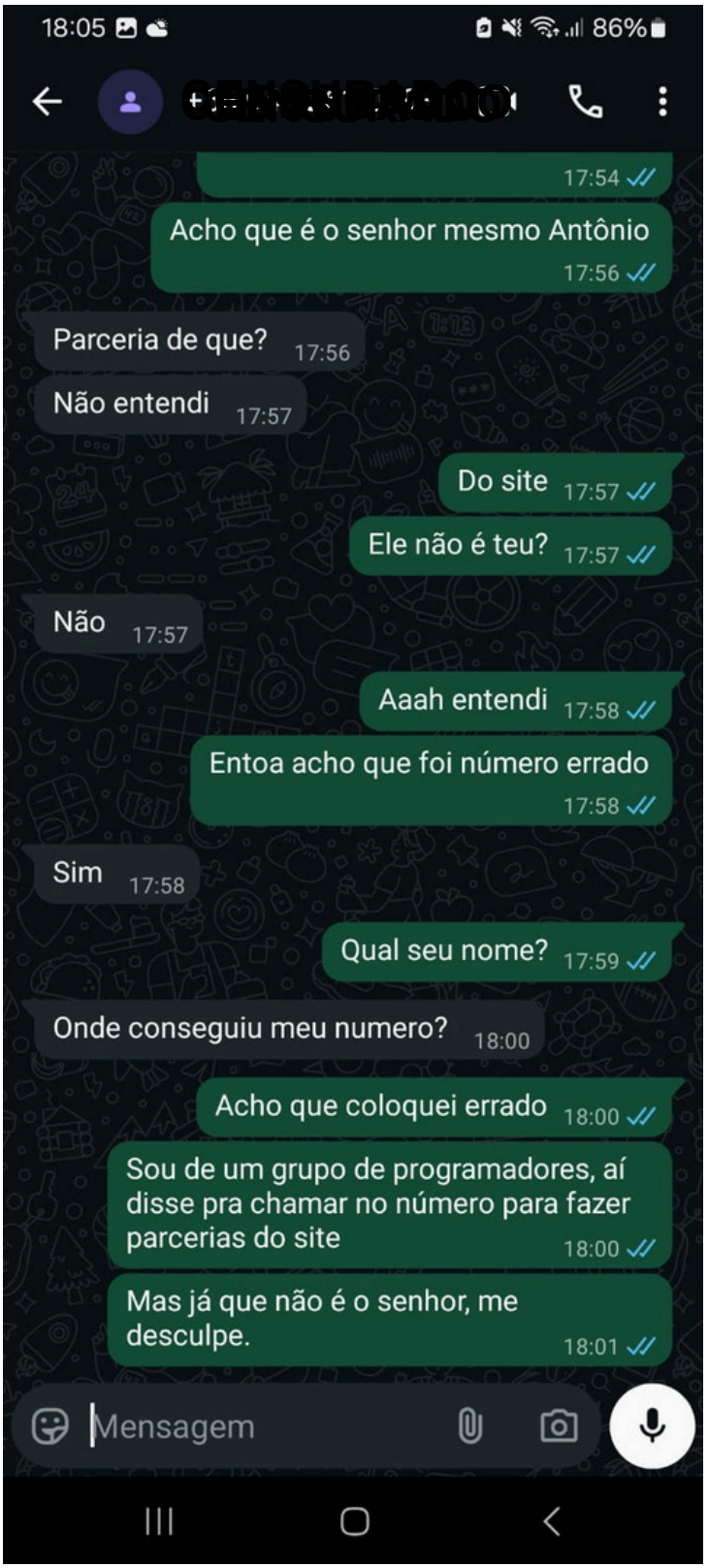
- Telefone de contato obtido via conversa WhatsApp: CENSURADO.
  E-mail associado (informado no site/conversa): CENSURADO.
- Endereço informacional (aparente): CENSURADO (possível dado falso).
- Nameservers observados no domínio: CENSURADO— indica uso de Cloudflare (CDN/proxy).
-
  Evidências (prints WhatsApp): duas imagens de conversa fornecidas:
- (As imagens mostram comunicações entre o atacante/operador e pessoa que tenta contato; servem como prova de operação e número usado para contato.)

Comportamento técnico observado: ao realizar a jornada de “pagamento” foi identificado um recurso que aponta para pix.adyen.com e fornece um token JWT que descreve dados de localização do QR Code PIX. Isso sugere integração (real ou simulada) com Adyen para gerar códigos de pagamento.

Observações: não foi disponibilizado diretamente o IP de hospedagem por conta do uso de Cloudflare como proxy. Recomendamos resolução DNS e consulta a histórico/passive DNS para identificar IPs de origem antes da proteção por Cloudflare (se houver).

Nível de risco: ALTO — evidência de interação com vítimas e fluxo de pagamento ativo.


18:05
86%
pessoas que fazem parte da conversa podem ler, ouvir e compartilhar esse conteúdo. Saiba mais
Olá seu Antonio boa noite tudoo bem?
Editada 17:51
Opa 17:51
Tudo bom? 17:53
Vi que você é dono de um site 17:53
Gostaria de fazer parceria 17:53
Mandou mensagem para pessoa errada 17:54
Aah, você não é Antônio? 17:54
Dono do site app.mercadodigital? 17:54
Acho que é o senhor mesmo Antônio 17:56
Parceria de que? 17:56
Não entendi 17:57
Do site 17:57
Ele não é teu? 17:57
Não 17:57
Mensagem


18:05
86%
17:54
Acho que é o senhor mesmo Antônio 17:56
Parceria de que? 17:56
Não entendi 17:57
Do site 17:57
Ele não é teu? 17:57
Não 17:57
Aaah entendi 17:58
Entoa acho que foi número errado 17:58
Sim 17:58
Qual seu nome? 17:59
Onde conseguiu meu numero? 18:00
Acho que coloquei errado 18:00
Sou de um grupo de programadores, aí disse pra chamar no número para fazer parcerias do site 18:00
Mas já que não é o senhor, me desculpe. 18:01
Mensagem

mercadooolivrrrcumpoo-app.com — Domínio de apoio à campanha

mercadooolivrrrcumpoo-app.com — Domínio de apoio à campanha

Classificação: Domínio de infraestrutura ou site satélite possivelmente usado na campanha.
WHOIS / Registro:

- *Data de criação: 17/09/2025.*
- *Registrador / Hospedagem: GoDaddy (informação do WHOIS).*
- *Endereço: [redacted] (endereço do serviço de proteção/privacidade).*
- *Nameservers: [redacted] (DNS da Cloudflare).*

Nível de risco: MÉDIO/ALTO — domínio recente, possivelmente usado em campanhas de anúncios; requer preservação de logs e histórico de DNS.

[redacted] — Domínio com registrar UOL Host

3.3 [redacted] — Domínio com registrar UOL Host

Classificação: Domínio com relação incerta. Possível uso em páginas de campanha ou suporte.

Registrador: Universo Online (UOL Host) (uolhost.com.br). Contato/telefone público do registrador disponível no RDAP/WHOIS.

Observação: registrante não identificado publicamente; requer pedido formal ao UOL Host para preservação de dados e identificação do registrante.

Nível de risco: MÉDIO — exige verificação adicional.

Análise técnica detalhada: Token JWT e fluxo PIX (vetor-chave)

Análise técnica detalhada: Token JWT e fluxo PIX (vetor-chave)

Descrição técnica (resumida): foi encontrado um token JWT associado ao recurso:

https://pix.adyen.com/pixqrcodelocation/pixloc/v1/loc/hNRYE05fQV-UKWVI7yKJbA

Ao acessar esse recurso, o servidor retorna/fornece um JWT que contém um payload com metadados relativos ao QR Code PIX — por exemplo, identificadores de localização, timestamps e possivelmente o identificador da instrução de pagamento. O JWT recebido (texto exato fornecido pela equipe) foi salvo como evidência.
Token (fornecido pela equipe):

Interpretação e risco:

- Um JWT não necessariamente indica que a Adyen é responsável pela conta recebedora; pode ser uma chamada legítima da API da Adyen se os golpistas usarem uma conta Adyen (autenticada) ou podem estar simulando o fluxo (ex.: hospedando conteúdo que retorna um JWT forjado).
- Em ambos os casos, o JWT facilita localizar a origem do QR Code e os parâmetros usados para pagamento — portanto, é uma peça chave de investigação.
- Se for uma integração legítima e as chaves/contas forem reais, a Adyen poderá relacionar o JWT/payload a uma conta recebedora, transações e logs (IP de criação, timestamp, conta bancária recebedora, etc.).
- Se for forjado, ainda é possível rastrear a infraestrutura que serve esse JWT (domínio, headers HTTP, certificados TLS, IPs de origem), ajudando a mapear os operadores.
-

Recomendação técnica imediata: encaminhar o JWT e a URL pix.adyen.com/pixqrcodelocation/... diretamente para o time de abuse/forensics da Adyen com pedido de auditoria dos logs para o identificador contido no payload (campo txid/txid-like/cnpj ou outro identificador), e pedir informações sobre a conta recebedora e IPs de criação do token.

IoCs (Indicators of Compromise) — listagem técnica pronta para ingestão

Domínios:

CENSURADO CENSURADO
CENSURADO CENSURADO
CENSURADO CENSURADO

URLs / Recursos:

CENSURADO CENSURADO
CENSURADO CENSURADO CENSURADO CENSURADO
JWT)

E-mails:

CENSURADO CENSURADO CENSURADO site)

Telefones:

CENSURADO CENSURADO CENSURADO operador/contato aparente)
Tokens / Artefatos (salvos como evidência):
CENSURADO CENSURADO SALVAR como evidencias/pix_jwt.txt.
Arquivos de evidência (prints):

CENSURADO CENSURADO
- prova 2.jpg

CENSURADO CENSURADO

Observações: não foram detectados hashes de executáveis/malware; se houver scripts / pacotes recebidos, incluir hashes e samples.

Avaliação de risco e priorização

- ALTO (prioridade 1): [redacted] — evidência de pagamento e contato com vítimas; JWT ligado a fluxo de pagamento (vetor para encontrar conta recebedora).
- ALTO/MÉDIO (prioridade 2): [redacted] — domínio recente hospedado em GoDaddy com nameservers Cloudflare — possível infraestrutura de suporte.
- MÉDIO (prioridade 3): [redacted] — registrado UOL Host, relação incerta; verificação necessária.

Prioridade operacional sugerida:

- Preservação e pedido de logs e identificação para Adyen (usando o JWT como evidência).
- Pedido de preservação de WHOIS e logs ao GoDaddy para o domínio criado em 17/09/2025.
- Pedido de preservação ao UOL Host para especialfimdeanoml.com.
- Notificação às plataformas de anúncio (Google Ads / Meta) para desativação/remoção das campanhas que estejam promovendo esses domínios.
- Comunicação às possíveis vítimas sobre como preservar provas (prints de comprovantes, conversas, dados bancários).

Recomendações práticas

- Ação imediata (preservação)
- Salvar todo o conteúdo das páginas com wget --mirror --convert-links --page-requisites --no-parent https://[redacted] e também capturar os HTMLs, imagens e HAR do navegador. Calcular hash dos arquivos.
- Exportar conversas (WhatsApp) em formato que preserve metadata e timestamps (se disponível).
- Criar cópia forense das evidências em mídia criptografada (ex.: disco externo com VeraCrypt) e anotar hashes.

Comandos e procedimentos úteis para replicação (técnico)

Obter whois / rdap:

whois app-mercadodigitalml.com
curl -s https://rdap.registrar.example/domain/app-mercadodigitalml.com

Resolver DNS/obter IP:

dig +short app-mercadodigitalml.com A
dig +trace app-mercadodigitalml.com

Baixar página para preservação:

wget --mirror --convert-links --adjust-extension --page-requisites --no-parent https://app-mercadodigitalml.com/

Decodificar JWT (localmente; não enviar chaves privadas):

decodificar header/payload (base64)
python3 -c "import sys,base64,json;
print(json.dumps(json.loads(base64.urlsafe_b64decode(sys.argv[1]+'==')), indent=2))" <payload_base64>

Gerar hash dos arquivos:

sha256sum prova\ 1.jpg
sha256sum prova\ 2.jpg
sha256sum prova\ 3.jpg
sha256sum pix_jwt.txt

Observações legais e éticas

- Toda coleta foi passiva e feita em fontes públicas; nenhuma ação de invasão, scanning intrusivo ou obtenção de dados protegidos foi executada.
- Para ações mais avançadas (logs, identificação de conta recebedora, scraping forense de servidores), recomenda-se solicitar formalmente aos provedores via seus canais de abuse/forensics ou por meio de ordem judicial, conforme a política do provedor e a legislação aplicável.
- Recomenda-se que a entidade civil coordene com um advogado ou setor jurídico para formalizar pedidos a provedores e redigir ofícios.

Próximos passos recomendados (sugestão operacional)

- Preservação imediata — salvar HTMLs, HAR, prints e JWT em mídia segura.
- Contato com Adyen — enviar JWT e pedir logs/transações associadas (prioridade máxima).
- Pedido de preservação ao GoDaddy — [illegible] CENSURADO CENSURADO Threat Intelligence
- Pedido de preservação ao [illegible] CENSURADO CENSURADO Threat Intelligence
- Notificação aos canais de anúncios (Google Ads / Meta) — para desativar campanhas e fornecer dados do anunciante.
- Bloqueio de páginas/URLs — quando confirmado, solicitar takedown (removal) via provedores/registrars.
- Comunicação às vítimas — orientar sobre preservação de provas e procedimento para eventual reembolso/denúncia.
- Registro formal dos dados de evidência — preencher e assinar formulário de cadeia de custódia.

Contato e assinatura

Ygor Costa — Pentester

Email: ygorcostax@outlook.com

WhatsApp: (24) 97403-9403

Natan Fagundes — Pentester/Dev Fullstack

Email: natanfagundes81@gmail.com

WhatsApp: (71) 8644-2301