# MadeiraMadeira + Axur: interrompendo o "golpe do imóvel por temporada"

Sobre a empresa

madeiramadeira

A maior loja online de móveis e decoração da América Latina. Com mais de 2000 colaboradores e 100 lojas físicas espalhadas pelo Brasil, democratiza o acesso a produtos de qualidade e oferece uma experiência completa de compra para transformar ambientes.

## Problema

Os criminosos buscavam informações vazadas, como cartões de crédito comprometidos ou logins encontrados em logs de malware. Com esses dados, conseguiam fazer login e realizar pedidos na loja. Em seguida, alugavam um imóvel por temporada para ter um endereço fictício e fazer o recebimento dos itens comprados. A MadeiraMadeira precisava de um monitoramento amplo e, principalmente, de mecanismos de Threat Intelligence para encontrar e interromper as fraudes antes que os chargebacks aumentassem ainda mais durante a Black Friday.

## Solução

Com o monitoramento de Deep & Dark Web da Axur, a MadeiraMadeira teve acesso às primeiras conversas entre threat actors divulgando esquemas fraudulentos. A equipe acompanhou de perto as menções à empresa por 30 dias para solucionar o problema.

Além das detecções automáticas, utilizaram a ferramenta Explorar, uma busca aberta nos milhares de grupos e fóruns do cibercrime, que permite uma abordagem proativa em investigações.

## Impacto em números

- 905K sinais monitorados entre dez/2022 e set/2023
- 21,8K ameaças encontradas no período
- 4,3K incidentes registrados e tratados
- 30 dias de investigação focada para desvendar o esquema
- Esquema interrompido com verificação de segurança

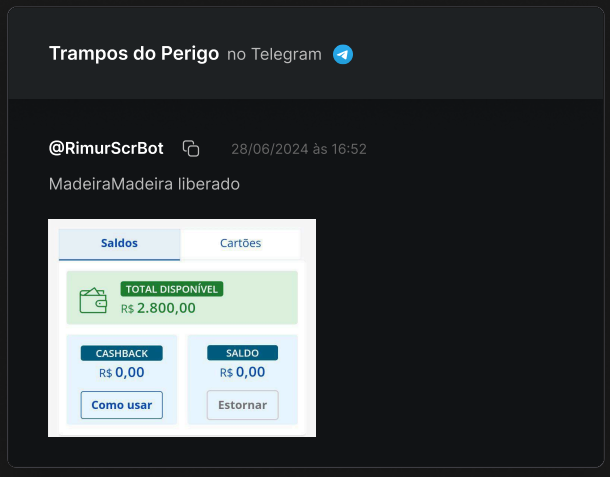



Imagem 1: Prints de golpista conversando sobre a MadeiraMadeira antes da parceria com a Axur

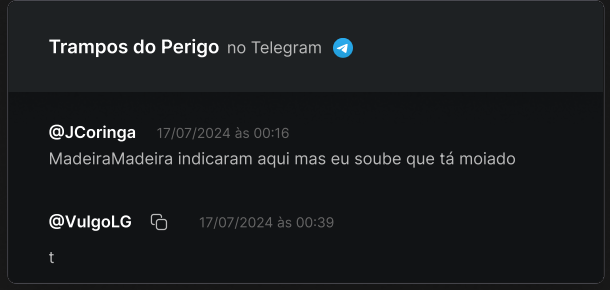



Imagem 2: Prints de golpistas reclamando após a parceria entre MadeiraMadeira e Axur

## Da incerteza aos insights: rastreando a raiz do problema

Com o apoio da Axur, a MadeiraMadeira identificou a origem de um esquema de fraude divulgado na Deep & Dark Web, onde criminosos compartilhavam instruções, endereços e comprovações de compras indevidas aprovadas. Antes, a empresa só reagia após os chargebacks, por falta de visibilidade dessas conversas.

## Ferramenta Explorar: busca proativa em tempo real

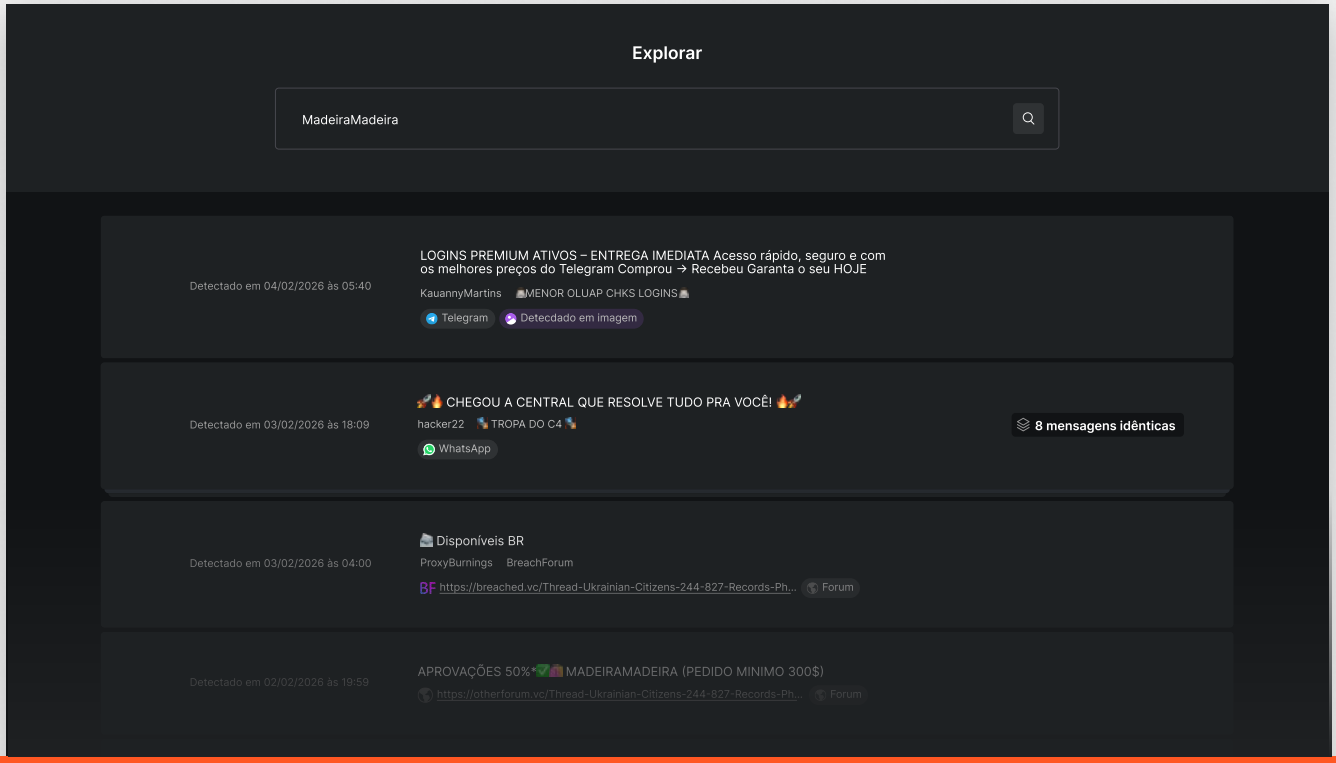
Com a ferramenta Explorar, a equipe acessou dados da Deep & Dark Web em tempo real, investigou conversas com contexto histórico, priorizou riscos e acionou respostas imediatas por meio de alertas inteligentes.

## Detecção multimídia revela esquema completo

A partir de OCR em imagens e transcrição de áudios e vídeos, foi possível mapear todo o golpe e implementar uma verificação de segurança para compras destinadas a imóveis por temporada, interrompendo o esquema de forma preventiva.

## Frustração dos fraudadores comprova eficácia

Após a implementação, fraudadores passaram a relatar dificuldades para concluir golpes, comprovando a eficácia da estratégia.
A MadeiraMadeira não apenas bloqueou o esquema identificado, como fortaleceu a proteção contínua contra novas tentativas, inclusive em períodos críticos como a Black Friday.




# Descubra, investigue e interrompa ameaças na Deep & Dark Web

AGENDE UMA DEMO

Gartner Peer Insights 4.9

Conheça todas as nossas soluções: **axur.com**

AXUR