CASO DE SUCESSO

Axur | MadeiraMadeira

Investigando o "golpe do imóvel por temporada" e interrompendo chargebacks

CASO DE SUCESSO

Axur + MadeiraMadeira

Como a Axur ajudou a MadeiraMadeira a investigar o “golpe do imóvel por temporada” e interromper os chargebacks

905K

Sinais monitorados pela Axur

21,8K

Ameaças encontradas

4,3K

Incidentes registrados

madeiramadeira

Sobre a empresa

A MadeiraMadeira é a maior loja online de móveis e decoração da América Latina

Indústria

E-commerce

Tamanho da empresa

Mais de 2000 colaboradores e 100 lojas físicas espalhadas pelo Brasil.

*dados referentes à cobertura total de monitoramento, entre dezembro/2022 e setembro/2023.

///AXUR

Como funcionava o golpe do imóvel por temporada

1. Os criminosos buscavam informações vazadas, como cartões de crédito comprometidos ou logins encontrados em logs de malware
2. Eles conseguiam fazer login e realizar pedidos na loja usando os dados encontrados
3. Então, alugavam um imóvel por temporada para ter um endereço fictício e, lá, faziam o recebimento dos itens comprados no site

Da incerteza aos insights: combatendo fraudes na Black Friday

1. A MadeiraMadeira precisava de uma forma de controlar os chargebacks de compras feitas em seu site por esquemas fraudulentos como o “golpe do imóvel por temporada”
2. Com a chegada do período da Black Friday, época do ano em que os e-commerces mais registram fraudes, a empresa antecipa que suas taxas de chargeback poderiam aumentar ainda mais
3. A loja precisava de um monitoramento amplo e, principalmente, de mecanismos de Threat Intelligence para encontrar e interromper as fraudes

Ao iniciar o trabalho com a Axur, a MadeiraMadeira conseguiu rastrear a raiz do problema que estava afetando suas operações.

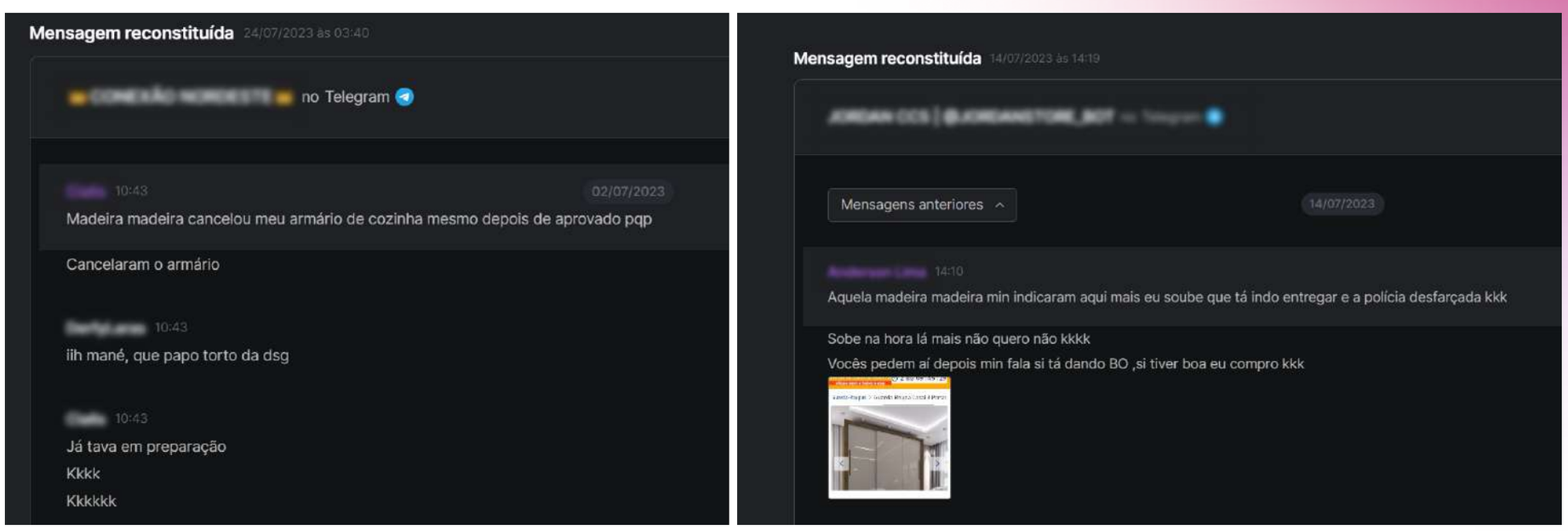
A investigação

A partir do monitoramento de Deep & Dark Web com a Axur, a MadeiraMadeira teve acesso às primeiras conversas entre threat actors divulgando os esquemas fraudulentos.

Além de divulgar como fazer a fraude e o endereço do imóvel alugado, os fraudadores se vangloriavam quando uma compra indevida era aprovada.

A equipe do MadeiraMadeira acompanhou de perto as menções à empresa na Deep & Dark Web por 30 dias para solucionar este problema. Além de acompanhar as detecções automáticas, também utilizaram a ferramenta Explorar, uma busca aberta nos milhares de grupos e fóruns do cibercrime, que permite uma abordagem pró-ativa em investigações.

Utilizando a tecnologia OCR que permite a detecção de menções em imagens, e as transcrições de áudios e vídeos nestes canais, a equipe conseguiu desvendar todo o esquema e adicionar uma verificação de segurança sempre que uma compra fosse solicitada para um endereço de imóvel por temporada.



Mensagens depois da investigação mostram a frustração e o medo dos fraudadores que estavam mencionando a marca

A gestão de ameaças é um desafio contínuo que necessita de acompanhamento 24×7 e recursos sofisticados para detectar fraudes e esquemas que são divulgados incessantemente na Deep & Dark Web.

> ***"É um produto muito importante, um dos melhores do mercado. Eu com certeza indicaria a Axur. Temos uma parceria muito boa"*** Bruno Silveira, Head de Segurança da Informação da MadeiraMadeira

Descubra, investigue e interrompa ameaças na Deep & Dark Web

A Axur coleta e processa automaticamente um grande volume de dados, gerando insights altamente relevantes através de curadoria, normalização, enriquecimento e avaliação de risco.

Receba alertas quando sua empresa, indústria ou palavras-chave escolhidas forem mencionadas ou quando padrões de anomalias previamente configurados forem identificados. Isso lhe permite priorizar ações com a rapidez necessária para reduzir a janela de oportunidade dos atacantes.

Inteligência de Ameaças

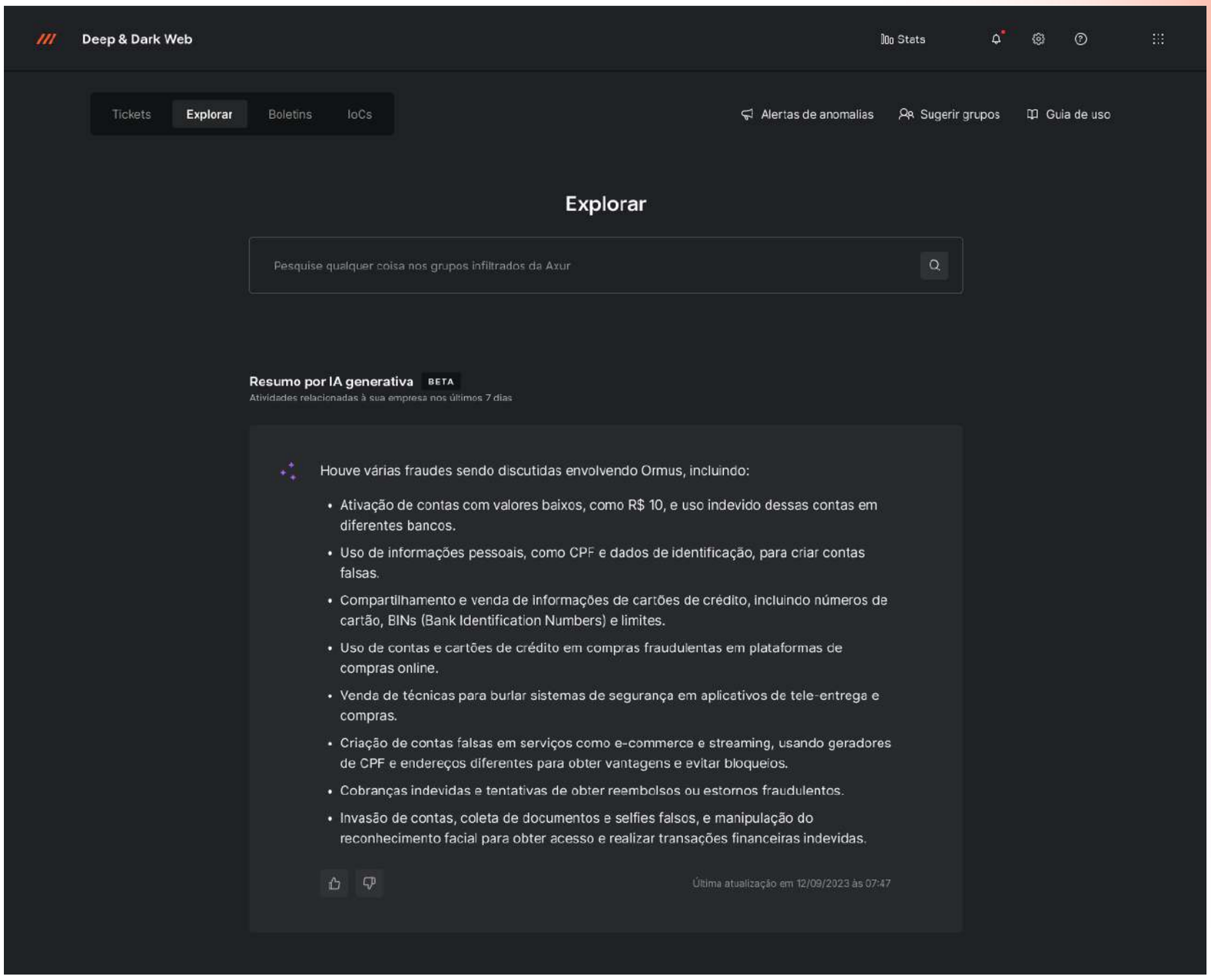
Antecipe ataques cibernéticos iminentes e solucione vulnerabilidades para prevenir ameaças. Receba nossos boletins de segurança e obtenha suporte da nossa equipe CTI em incidentes, com apoio em investigações e interações com threat actors.

Revele novos esquemas e detecte fraudes

Descubra ameaças ao seu negócio, indústria e concorrentes com pesquisas personalizadas. Identifique Técnicas, Táticas e Procedimentos (TTPs), gerencie riscos, cumpra as regulamentações de proteção de dados e mantenha-se vigilante contra golpes e atividades fraudulentas.

Explorar

Pesquise qualquer coisa no maior repositório integrado de dados brutos da Deep & Dark Web, com acesso ao conteúdo dos fóruns do cibercrime em um ambiente totalmente seguro.



///AXUR

Monitore o WhatsApp, Telegram, Discord, Fóruns e Mercados da Deep & Dark Web e diversos sites da Darknet

- Detecte conteúdo dentro de imagens, áudio e anexos de vídeo;
- Filtre resultados por relevância, data ou predefinições personalizadas, acionando alertas para novas descobertas;
- Navegue por mensagens passadas e futuras para obter contexto de conversas;
- Crie tickets de ação para os casos mais críticos, permitindo investigação imediata;
- Otimize a eficiência agrupando mensagens idênticas postadas em diversos canais.

Experimente a plataforma Axur
Agende uma demo

Tire suas dúvidas
Converse com um especialista
Ou escreva para: contato@axur.com