AXUR

SUCCESS STORY

Axur | MadeiraMadeira

How Axur Helped MadeiraMadeira Investigate the "Seasonal Property Scam" and Prevent Chargebacks

SUCCESS STORY

Axur + MadeiraMadeira

How Axur Helped MadeiraMadeira Investigate the "Seasonal Property Scam" and Prevent Chargebacks

905K

Signals Monitored by Axur

21,8K

Threats Identified

4,3K

Incidents Recorded

madeiramadeira

About the Company

MadeiraMadeira is Latin America's largest online furniture and decoration store.

Industry

E-commerce

Company Size

Over 2000 employees and 100 physical stores across Brazil.

*data related to the total monitoring coverage, between December 2022 and September 2023.

///AXUR

How the Seasonal Property Scam Operated

1. Criminals sought leaked information, such as compromised credit cards or logins found in malware logs.
2. They could log in and place orders in the store using the acquired data.
3. Then, they rented a seasonal property with a fictitious address and received the purchased items there.

From Uncertainty to Insights: Combating Frauds on Black Friday

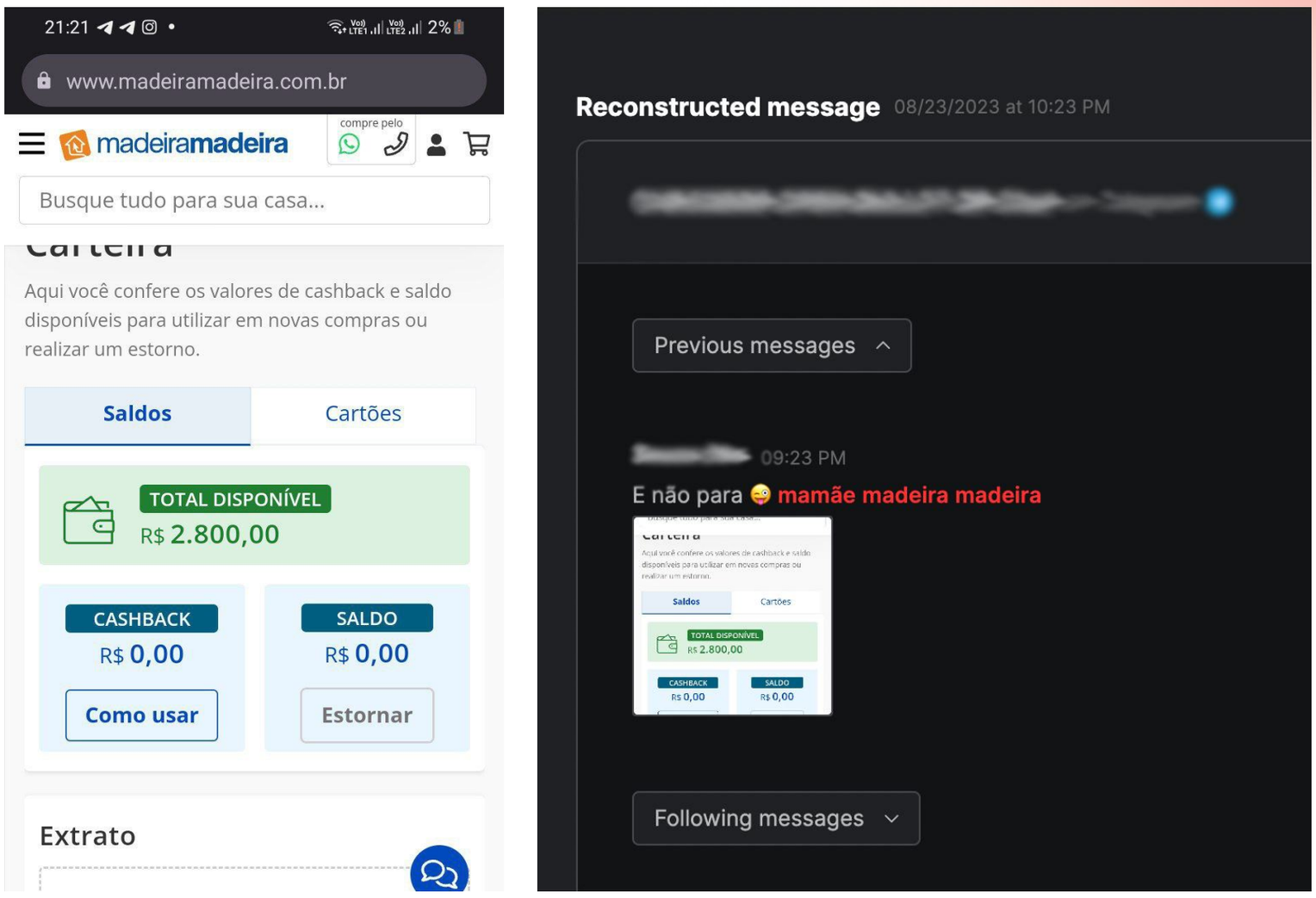
1. MadeiraMadeira needed a way to control chargebacks for purchases made on its website through fraudulent schemes like the "seasonal property scam."
2. With the approach of Black Friday, a time of the year when e-commerce platforms experience higher fraud rates, the company anticipated that its chargeback rates could increase even more.
3. The store needed comprehensive monitoring and, importantly, Threat Intelligence mechanisms to identify and halt fraud.

By partnering with Axur, MadeiraMadeira traced the root of the problem affecting its operations.

The Investigation

Through monitoring the Deep & Dark Web with Axur, MadeiraMadeira gained access to initial conversations among threat actors disclosing fraudulent schemes.

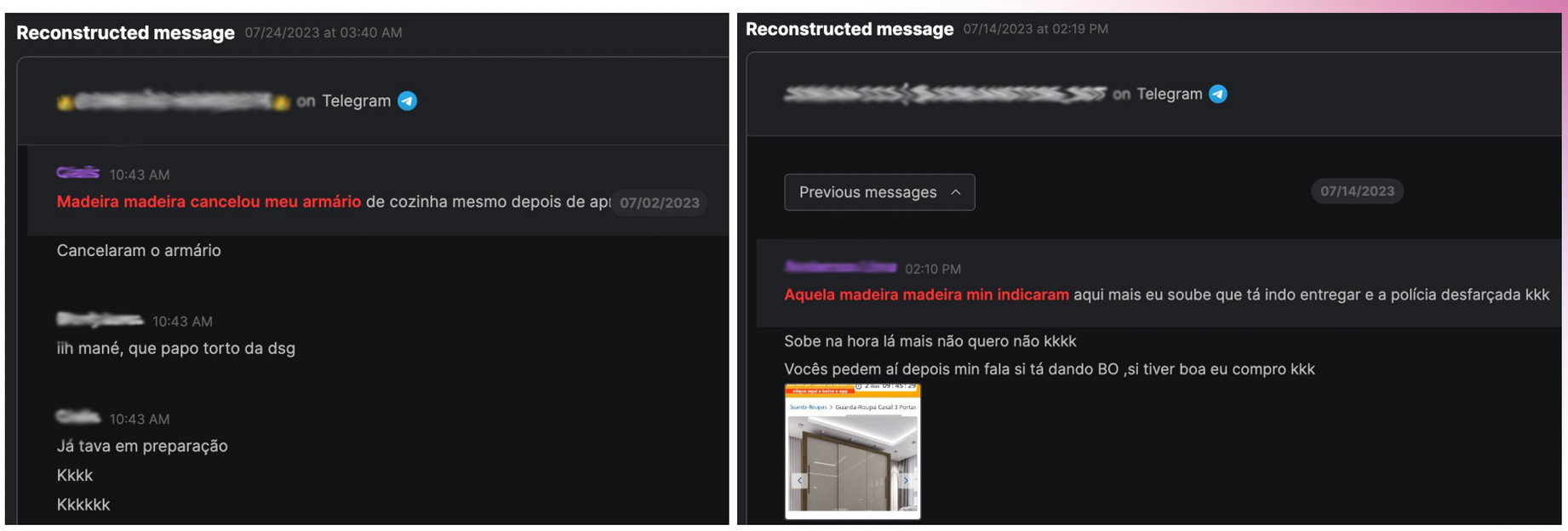
In addition to revealing how to commit fraud and the address of the rented property, fraudsters bragged when an unauthorized purchase was approved.



Messages detected by the Axur platform show disclosures of fraudulent schemes.

The MadeiraMadeira team closely monitored mentions of the company on the Deep & Dark Web for 30 days to resolve this issue. In addition to tracking automatic detections, they also used the Explore tool, an open search across thousands of cybercrime groups and forums, enabling a proactive approach to investigations.

Using OCR technology that detects mentions in images and transcriptions of audio and videos in these channels, the team unraveled the entire scheme and added a security check whenever a purchase was requested for a seasonal property address.



Messages after the investigation show the frustration and fear of fraudsters mentioning the brand.

Threat management is a continuous challenge that requires 24×7 monitoring and sophisticated resources to detect frauds and schemes that are incessantly disclosed on the Deep & Dark Web.

> ***"It's a critical product, one of the best on the market. I would definitely recommend Axur. We have an excellent partnership."***
> Bruno Silveira, Head of Information Security at MadeiraMadeira

Discover, Investigate, and Halt Threats on the Deep & Dark Web

Axur collects and automatically processes a large volume of data, generating highly relevant insights through curation, normalization, enrichment, and risk assessment.

Receive alerts when your company, industry, or chosen keywords are mentioned or when previously configured anomaly patterns are identified. This allows you to prioritize actions quickly to reduce the attackers' window of opportunity.

.

Threat Intelligence

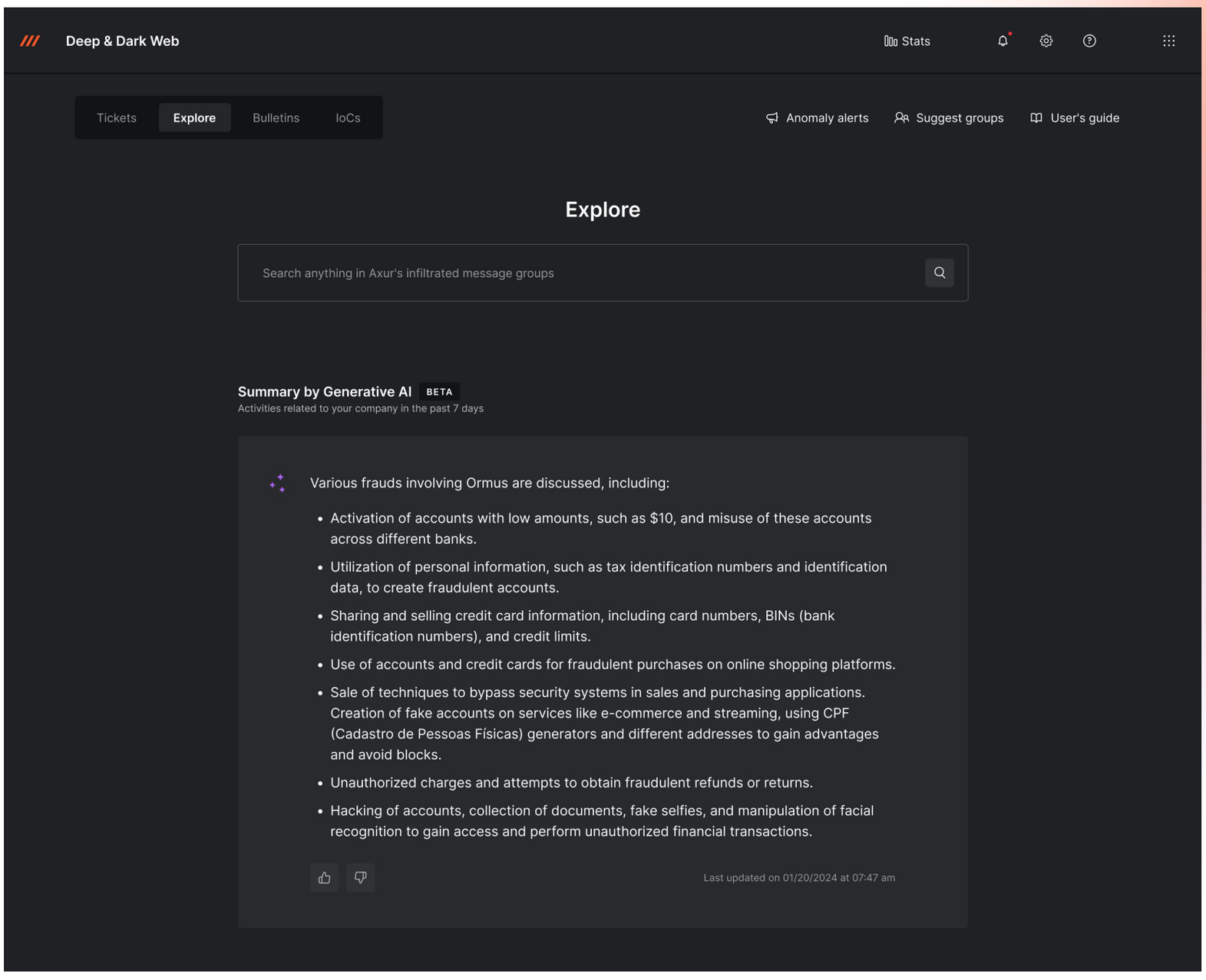
Anticipate imminent cyber attacks and address vulnerabilities to prevent threats. Receive our security bulletins and get support from our CTI team in incidents, with assistance in investigations and interactions with threat actors.

Uncover new schemes and detect frauds

Discover threats to your business, industry, and competitors with custom searches. Identify Techniques, Tactics, and Procedures (TTPs), manage risks, comply with data protection regulations, and stay vigilant against scams and fraudulent activities.

EXPLORE

Search anything in the largest integrated repository of raw data from the Deep & Dark Web, with access to the content of cybercrime forums in a fully secure environment.



///AXUR

Monitor WhatsApp, Telegram, Discord, Deep & Dark Web Forums, Markets, and various Darknet sites

- Detect content within images, audio, and video attachments.
- Filter results by relevance, date, or custom presets, triggering alerts for new discoveries.
- Browse past and future messages for conversation context.
- Create action tickets for the most critical cases, allowing immediate investigation.
- Optimize efficiency by grouping identical messages posted in various channels.

Experience the Axur platform
Schedule a demo

Clarify your doubts
Talk to an expert
Or write to contact@axur.com