MadeiraMadeira + Axur: interrumpiendo la “estafa del alquiler temporal”

Sobre la empresa

madeiramadeira

La mayor tienda online de muebles y decoración de América Latina. Con más de 2.000 colaboradores y 100 tiendas físicas distribuidas en Brasil, la empresa democratiza el acceso a productos de calidad y ofrece una experiencia de compra integral para transformar ambientes.

ProblemA

Los delincuentes buscaban información filtrada, como tarjetas de crédito comprometidas o credenciales encontradas en logs de malware. Con estos datos, lograban iniciar sesión y realizar pedidos en la tienda. Posteriormente, alquilaban inmuebles por temporada para utilizar direcciones ficticias y recibir los productos adquiridos. MadeiraMadeira necesitaba un monitoreo amplio y, principalmente, capacidades de Threat Intelligence para identificar e interrumpir los fraudes antes de que los chargebacks aumentaran aún más durante el Black Friday.

Solución

Con el monitoreo de Deep & Dark Web de Axur, MadeiraMadeira accedió a las primeras conversaciones entre actores maliciosos que divulgaban esquemas de fraude. El equipo realizó un seguimiento cercano de las menciones a la empresa durante 30 días para resolver el problema. Además de las detecciones automáticas, utilizaron la herramienta Explorar, un motor de búsqueda abierto en miles de grupos y foros de cibercrimen, que permite un enfoque proactivo en las investigaciones.

Impacto en cifras

- 905 mil señales monitoreadas entre 12/2022 y 11/2023
- 21,8 mil amenazas identificadas en el período
- 4,3 mil incidentes registrados y gestionados
- 30 días de investigación focalizada para desmantelar el esquema
- Esquema interrumpido con verificación de seguridad implementada

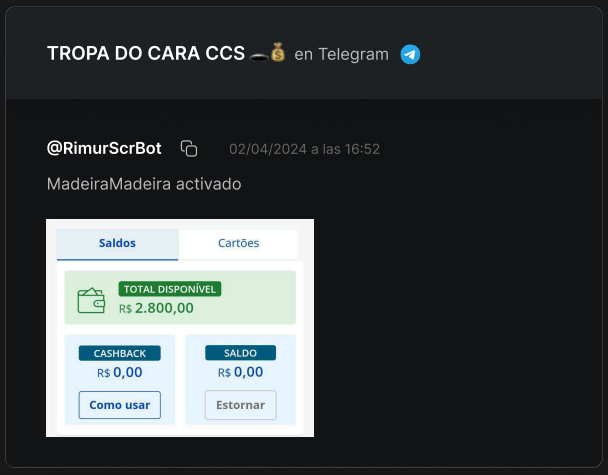


Imagen 1: Capturas de pantalla de un estafador hablando de MadeiraMadeira antes de la asociación con Axur.

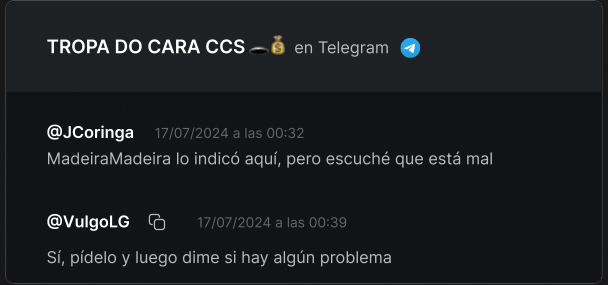


Imagen 2: Capturas de pantalla de estafadores quejándose tras la asociación entre MadeiraMadeira y Axur.

De la incertidumbre a los insights: rastreando la raíz del problema

Con el apoyo de Axur, MadeiraMadeira identificó el origen de un esquema de fraude divulgado en la Deep & Dark Web, donde los criminales compartían instrucciones, direcciones y comprobantes de compras fraudulentas aprobadas. Anteriormente, la empresa solo reaccionaba después de los chargebacks, debido a la falta de visibilidad sobre estas conversaciones.

Explorar: búsqueda proactiva en tiempo real

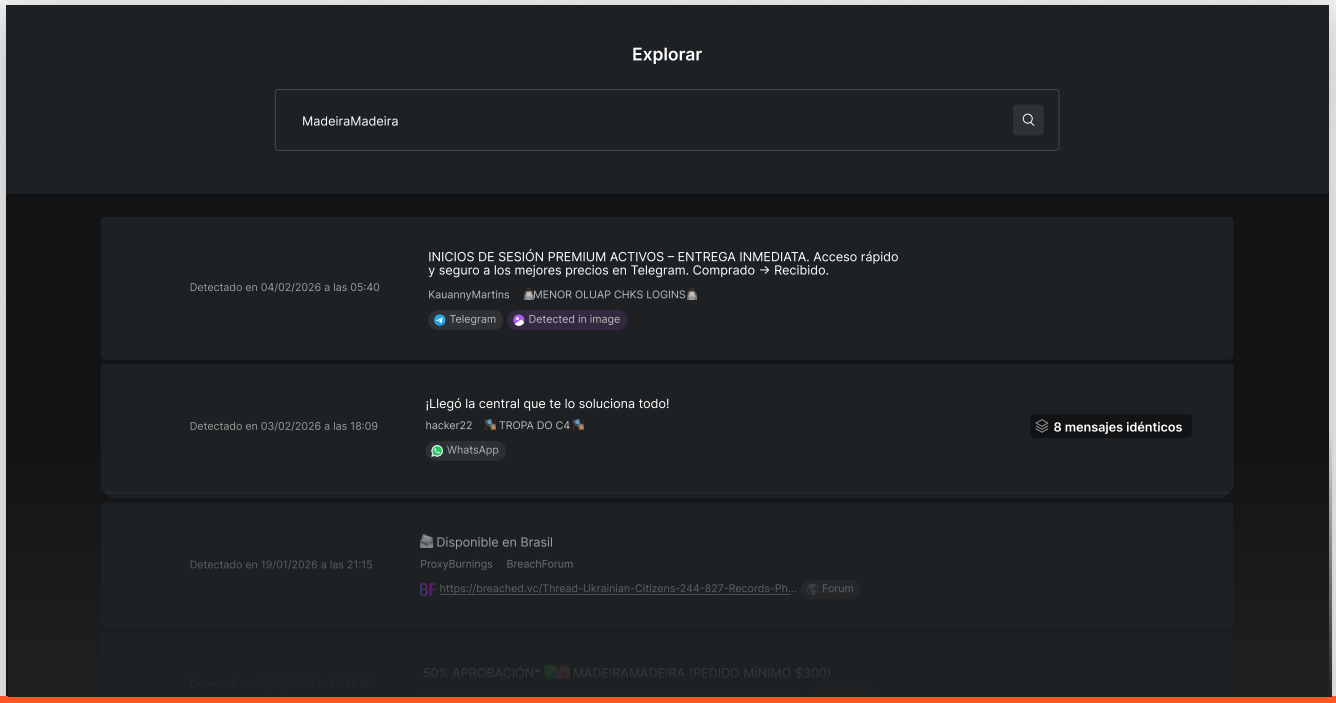
Con la herramienta Explorar, el equipo accedió a datos de la Deep & Dark Web en tiempo real, investigó conversaciones con contexto histórico, priorizó riesgos y activó respuestas inmediatas a través de alertas inteligentes.

Detección multimedia revela el esquema completo

Mediante OCR en imágenes y la transcripción de audios y videos, fue posible mapear el fraude en su totalidad e implementar una verificación de seguridad para compras destinadas a inmuebles por temporada, interrumpiendo el esquema de forma preventiva.

Frustración de los defraudadores confirma la eficacia

Tras la implementación, los defraudadores comenzaron a reportar dificultades para concretar las estafas, lo que confirmó la efectividad de la estrategia. MadeiraMadeira no solo bloqueó el esquema identificado, sino que también fortaleció la protección continua contra nuevos intentos, incluso durante períodos críticos como el Black Friday.



Descubra, investigue e interrumpa amenazas en la Deep & Dark Web

AGENDE UNA DEMO

Gartner Peer Insights 4.9

Conozca todas nuestras soluciones: **axur.com**

///AXUR