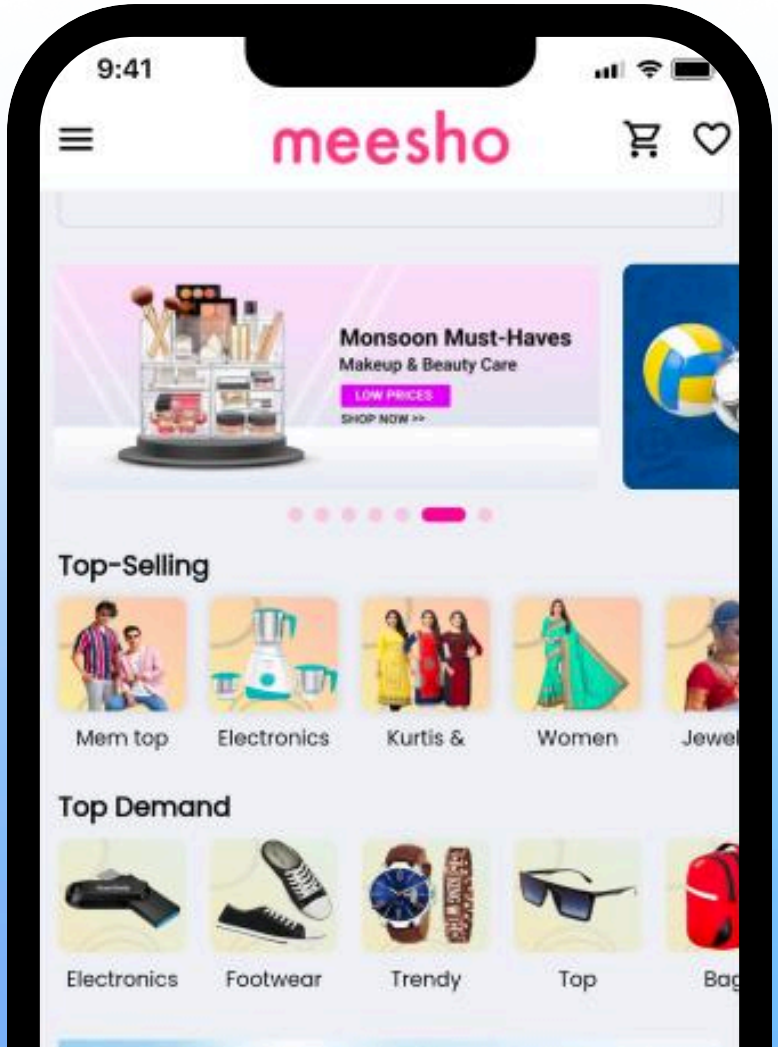
SHIELD | meesho

E-Commerce & Marketplace

Como a SHIELD ajuda Meesho a eliminar fraude com plataforma de inteligência de fraude focada na identificação de dispositivos

Meesho é uma plataforma indiana de social commerce com mais de 120M de usuários ativos mensais. A empresa conecta fornecedores, revendedores e consumidores, oferecendo uma maneira prática para que indivíduos ingressem no universo do e-commerce.

A plataforma de inteligência de fraude focada na identificação de dispositivos da SHIELD combina detecta a raiz da fraude por meio do **SHIELD Device ID** e retornamos inteligência acionável em tempo real, ajudando a Meesho a eliminar fraudes.

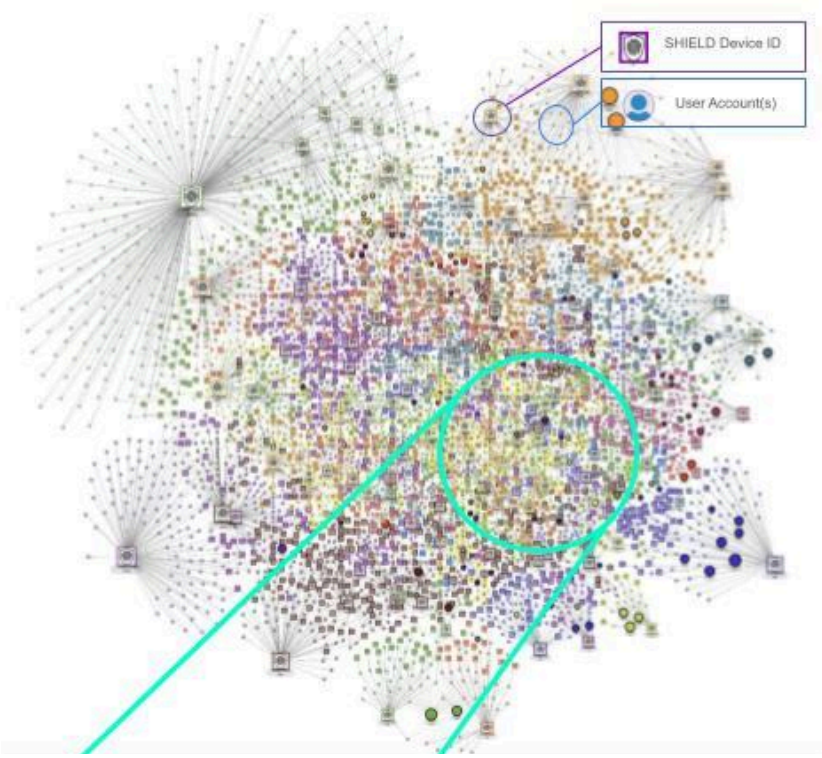


Casos de Uso

Fraude Interna & de Parceiros de Entrega

O que é fraude interna & de parceiros de entrega?

Entregadores e parceiros fraudulentos podem agir em conluio para roubar pacotes e produtos dos usuários e revendê-los, substituindo os itens por produtos defeituosos. Dessa forma, conseguem receber taxas de delivery sem realizar a entrega real da mercadoria.



SHIELD Fraud Intelligence

Uso de App Cloners
Uso de VPN
Reset de Fábrica Suspeito
Hooking
Screen-sharing

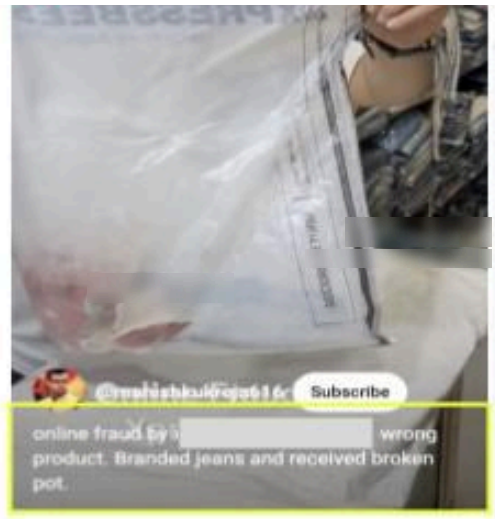
Observações

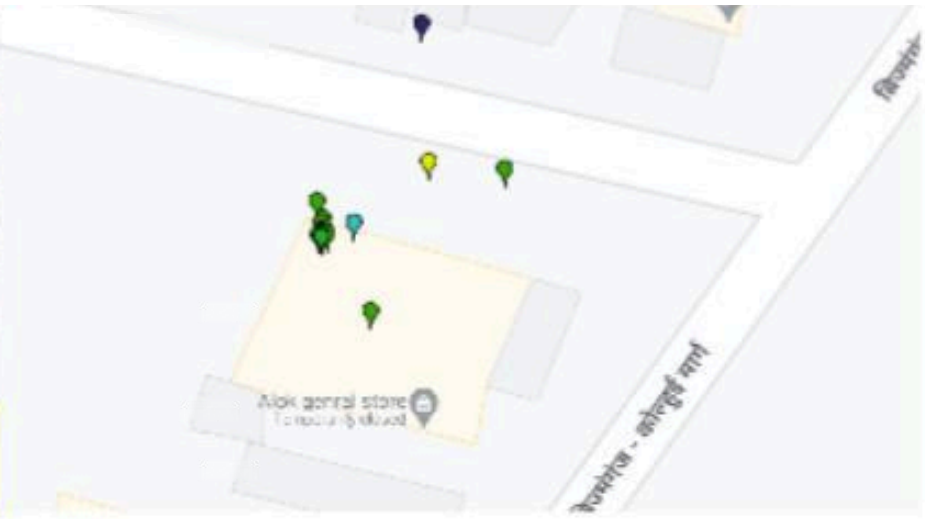
- **2,929 Dispositivos** controlados
- **4,094 contas de usuários**

Normalmente, **clonadores de apps** são utilizados para criar contas falsas em larga escala.

Essas contas falsas também são usadas para gerar avaliações e reviews fraudulentos, aumentando o ranking de anúncios e enganando usuários legítimos.

A SHIELD identificou **15 dispositivos** controlando 87 contas de usuários conectadas à rede Wi-Fi de parceiros logísticos de um cliente. A localização dos dispositivos apontava para um centro logístico parceiro.





**Todos os dados foram randomizados*

Casos de Uso

Conluio entre Comprador-Vendedor

O que é conluio entre comprador-vendedor?

Fraudadores criam tanto contas de compradores quanto de vendedores. Eles utilizam anúncios falsos para enganar usuários legítimos e vender produtos falsificados ou defeituosos, enquanto usam contas falsas para inflar artificialmente avaliações e melhorar o posicionamento desses anúncios.

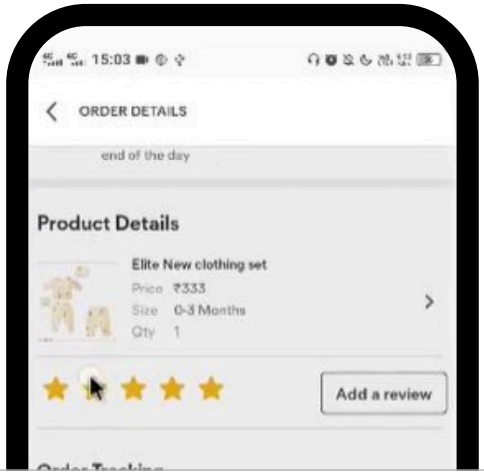
Usuários também podem receber cashback ou recompensas em marketplaces. Fraudadores entram em conluio com vendedores para abusar desses programas: realizam uma compra, recebem a recompensa e o vendedor devolve o valor do produto, fazendo com que nenhum dinheiro seja efetivamente gasto, mas os benefícios sejam obtidos. Depois, usuário e vendedor dividem os ganhos.

Fake Reviews

O que são fake reviews?

Fraudadores frequentemente criam contas falsas em escala para gerar avaliações fraudulentas e aumentar a visibilidade de anúncios falsos.

- O **SHIELD Device ID** identifica dispositivos vinculados a múltiplas contas de usuários.
- Já o **Fraud Intelligence** da SHIELD detecta ferramentas e técnicas utilizadas para acelerar a criação de reviews falsos, como clonadores de aplicativos e auto clickers.



Anúncios & Produtos Falsos

O que são anúncios & produtos falsos?

Fraudadores criam contas falsas para se passarem por afiliados legítimos de marcas e vender produtos falsificados ou de baixa qualidade.

- O **SHIELD Device ID** identifica dispositivos associados a múltiplas contas
- Já o **Fraud Intelligence** da SHIELD detecta ferramentas amplamente utilizadas para criar anúncios falsos em escala, como clonadores de aplicativos e emuladores.

Casos de Uso

Abuso de Promoção

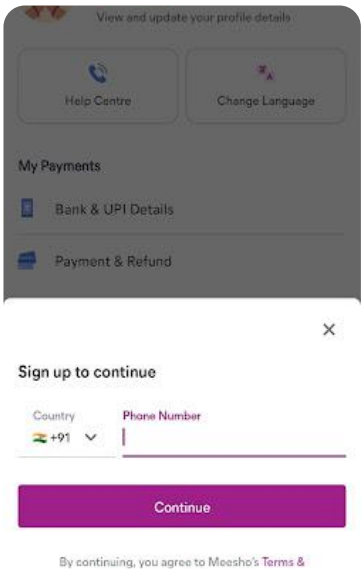
O que é Abuso de Promoção?

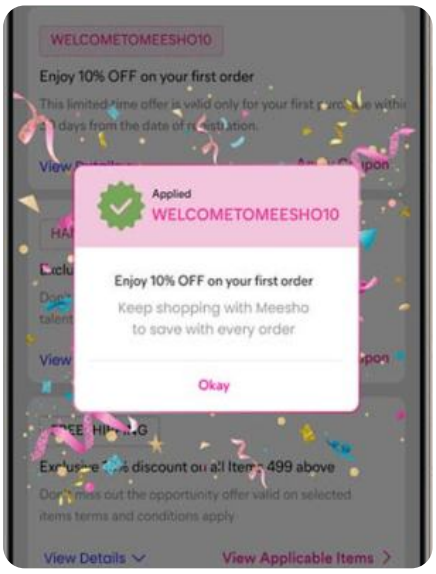
Fraudadores podem criar múltiplas contas falsas para resgatar os mesmos descontos repetidamente, consumindo orçamentos de campanhas promocionais. Eles também podem explorar bônus de cadastro para novos usuários e códigos de indicação da mesma forma. A SHIELD identifica dispositivos vinculados a múltiplas contas de usuários e detecta ferramentas utilizadas por fraudadores para automatizar e escalar esse processo.

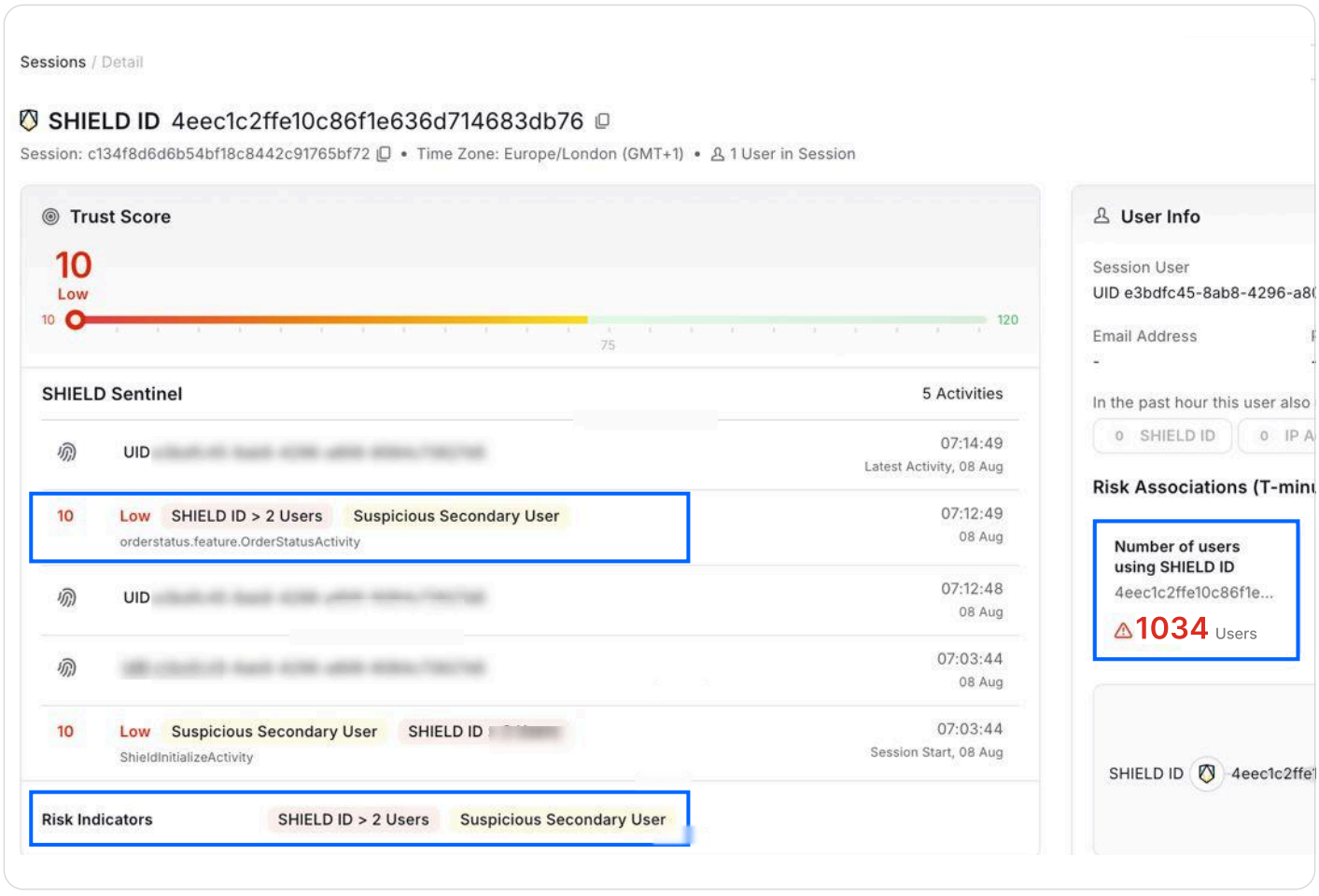
SHIELD Fraud Intelligence

A solução detecta ferramentas e técnicas amplamente utilizadas para acelerar o resgate de promoções, como clonadores de aplicativos e apps adulterados.

Essas ferramentas maliciosas são usadas para alterar atributos do dispositivo, permitindo que fraudadores evitem detecção e criem múltiplas contas em escala para abusar de bônus de cadastro, programas de indicação e descontos por tempo limitado.







Todos os dados foram randomizados

Casos de Uso

Account Takeover (Abuso de Serviços de Acessibilidade)

O que é Account Takeover (Abuso de Serviços de Acessibilidade)?

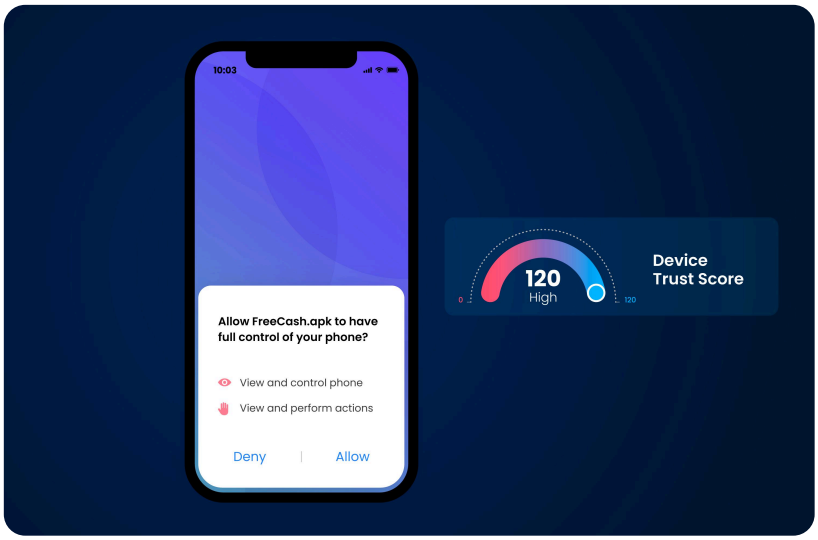
Vítimas podem, sem perceber, baixar aplicativos fraudulentos e conceder permissões de acessibilidade a eles. Quando isso acontece, fraudadores conseguem obter acesso remoto ao dispositivo, roubando dados de login, teclas digitadas, OTPs e muito mais. Esse método de Account Takeover (ATO) já foi utilizado para fraudar diversos usuários, incluindo celebridades e autoridades governamentais.

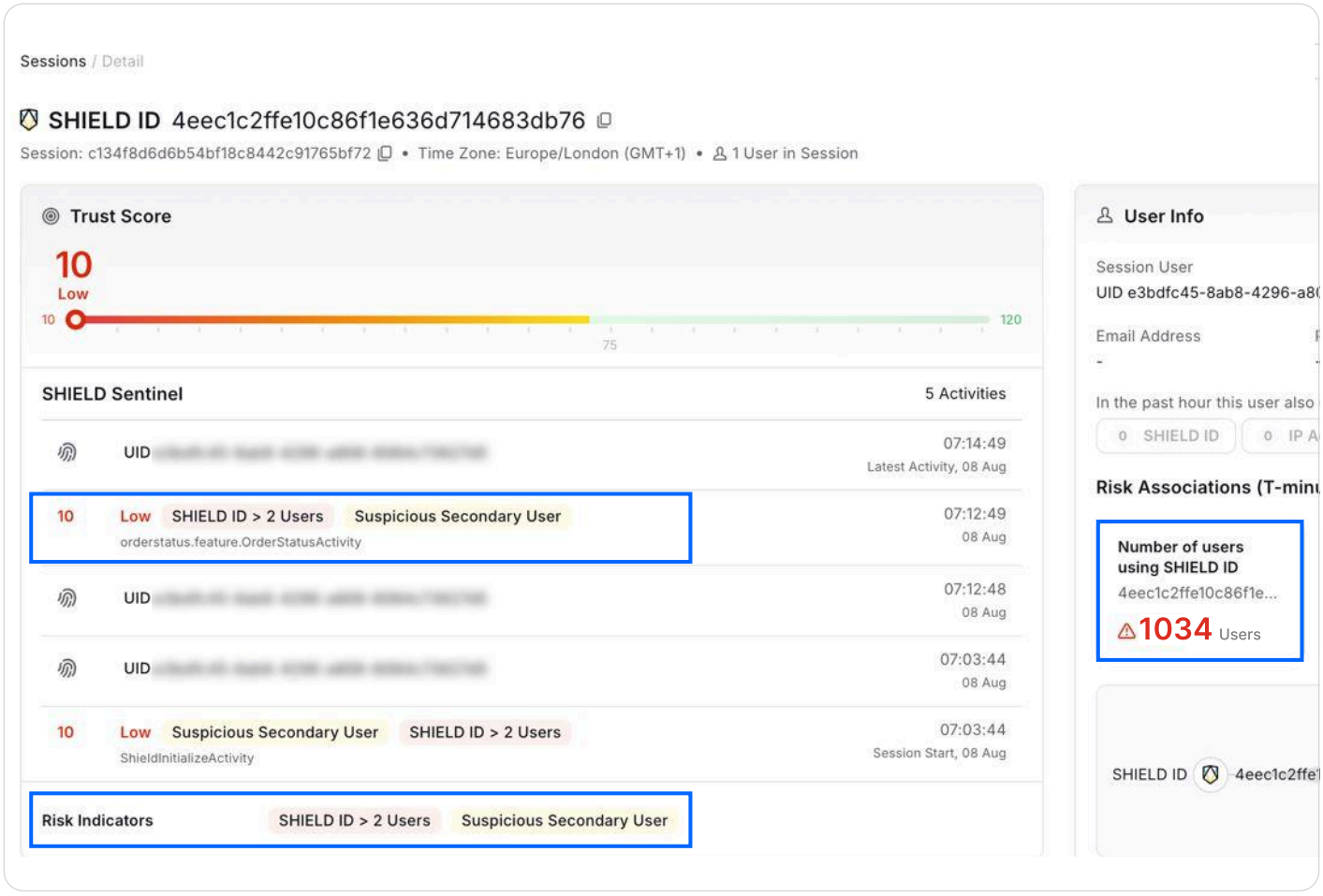
SHIELD Fraud Intelligence

O Fraud Intelligence da SHIELD monitora sessões dos dispositivos, identificando quando um usuário legítimo passa a apresentar comportamentos maliciosos.

Por exemplo, a SHIELD consegue detectar quando dispositivos com histórico consistente de confiança começam a exibir sinais suspeitos, incluindo:

- uso de ferramentas de **compartilhamento de tela** e **auto-clickers** - utilizadas por fraudadores especializados em ATO.





Casos de Uso

Account Takeover

O que é Account Takeover?

Fraude de Account Takeover (ATO) acontece quando fraudadores obtêm acesso não autorizado a contas de usuários utilizando credenciais roubadas. Eles utilizam técnicas como credential stuffing e ataques de força bruta para realizar invasões em massa. Após obter acesso às contas, conseguem executar diversos tipos de fraude, incluindo fraudes de pagamento e roubo de informações pessoais.

01

Fraude de Pagamento

Com acesso às contas, fraudadores podem roubar dados, incluindo informações de cartões de crédito, utilizando esses dados para realizar transações não autorizadas.

02

Fraude de Reembolso

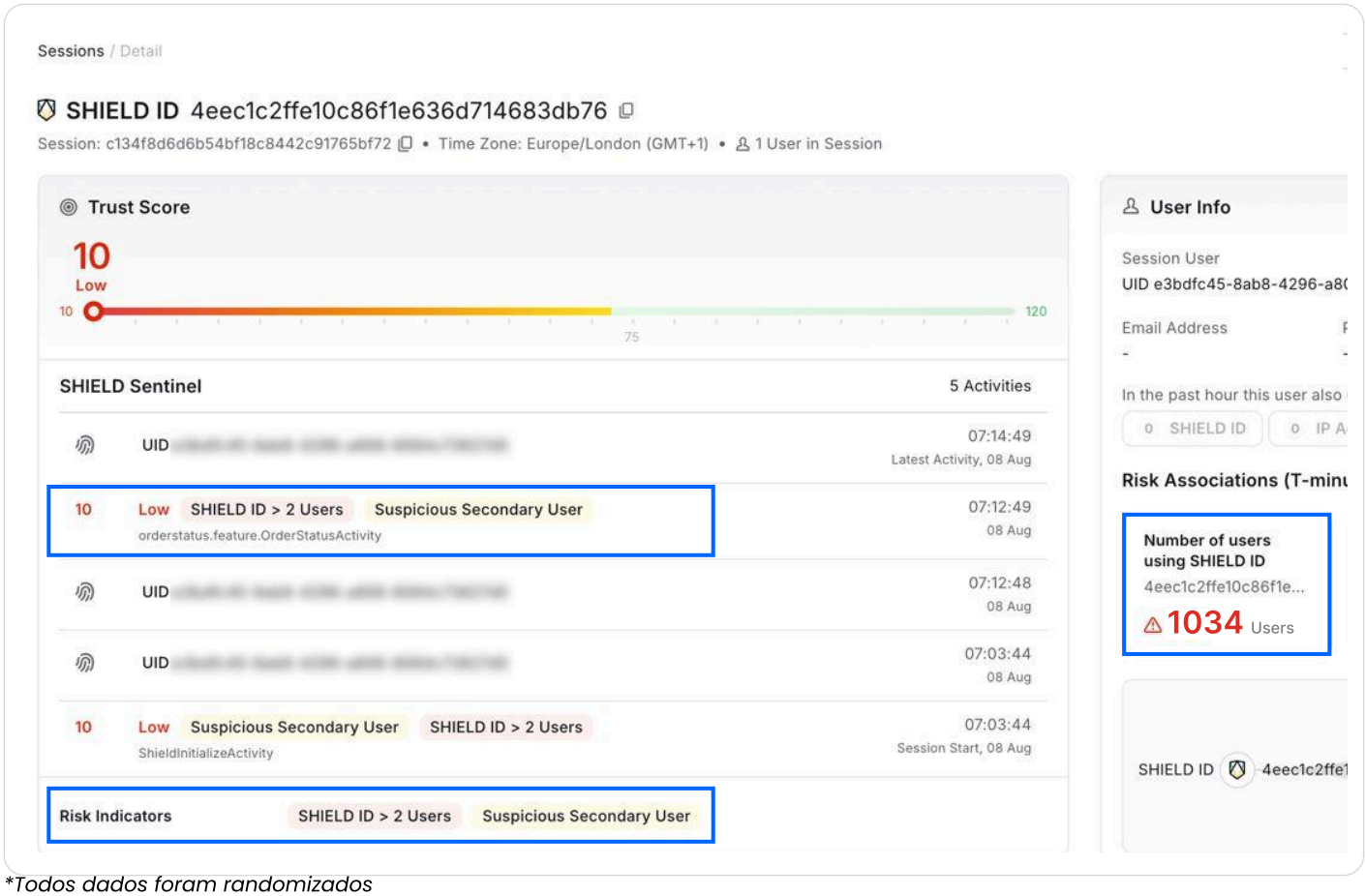
Fraudadores alteram dados bancários ou informações de cartão das vítimas sem seu conhecimento para desviar reembolsos realizados pelas plataformas.

SHIELD Fraud Intelligence

A SHIELD detecta quando múltiplas contas estão sendo acessadas por um mesmo dispositivo — um forte sinal de tentativa de ATO.

Também identifica múltiplas tentativas de login em curtos períodos de tempo e em diferentes localizações, classificando esse comportamento como atividade suspeita.

Além disso, a SHIELD detecta ferramentas e técnicas utilizadas para acelerar ataques de ATO, como emuladores e dispositivos com jailbreak/root.



*Todos dados foram randomizados