CASE STUDY

20-4

FINTECH CASHPLUS ADOTA SOLUÇÃO TRANSUNION E IMPEDE ATAQUE DE BOTS

Empresa: Cashplus, uma das Fintechs mais inovadoras do mundo

Segmento: Fintech

Produto/Solução: Device Risk | TruValidate

DESAFIO

Cerca de 9.500 pedidos fraudulentos de cartão inundaram a Cashplus em poucos dias. Os dados pessoais dos solicitantes passaram pela inspeção do provedor KYC (Know Your Customer). Os scripts de ataque variavam de endereços de IP de diferentes países por meio de VPNs. Incluir todos em uma lista restritiva seria inviável para os negócios.

A SOLUÇÃO

O Device Risk, da TransUnion, revelou uma brecha nos ataques - todas as solicitações usavam um mesmo tipo de dispositivo. Essa constatação levou a uma mudança no processo de pedidos da FinTech, que barrou o ataque permanentemente.

RESULTADOS

Assumindo o valor de £21 por transação, a Cashplus economizou £19.000 em taxas de serviço KYC e impediu a abertura de linhas de crédito para contas fraudulentas no valor de £2.000 cada. A FinTech alertou as vítimas cujas informações pessoais foram usadas nos pedidos, evitando a perda de milhões de libras decorrentes de roubo de identidade.

cashplus®

O RECONHECIMENTO DE DISPOSITIVOS DESEMPENHOU UM PAPEL FUNDAMENTAL NO ISOLAMENTO E NO BLOQUEIO DE 9.500 PEDIDOS FRAUDULENTOS.

"DESDE QUE ADOTAMOS A SOLUÇÃO TRUVALIDATE USAMOS SEUS DIVERSOS ELEMENTOS PARA ENRIQUECER NOSSOS DADOS INTERNOS E APRIMORAR NOSSA CAPACIDADE DE DETECÇÃO DE FRAUDES".

Paul Schooley, diretor operacional da Cashplus

Os primeiros 2.000 pedidos fraudulentos de cartão apareceram da noite para o dia. O nome, o endereço e a data de nascimento dos solicitantes estavam corretos. No entanto, os endereços de e-mail seguiam um padrão - e nenhum dos números de telefone estava em operação. Claramente, o endereço IP de referência precisaria ir para a lista restritiva.

Na manhã seguinte, chegou à FinTech outra onda de milhares de pedidos fraudulentos. Dessa vez, as solicitações vieram através de vários endereços IP, via diversas VPNs e de diferentes países.

Para a Cashplus, uma das FinTechs mais inovadoras do Reino Unido, que conhecia bem os esforços de fraudadores, o pico de atividade era incomum.

"Era um bot que estava apenas variando os detalhes para randomizar o ataque", explica James Coveney, gerente da área de fraudes e crédito da Cashplus. "Contando com os dados do Device Risk, parte da solução TruValidate da TransUnion, pudemos identificar um mesmo tipo de dispositivo em todos os pedidos. Combinamos esses dados com os nossos e fomos capazes de impedir que as solicitações fossem convertidas em contas de débito".

No momento em que a Cashplus interrompeu o ataque, os bots já haviam enviado 9.500 pedidos fraudulentos de cartão.

"O TRUVALIDATE NOS FORNECE DADOS AOS QUAIS NÃO TERÍAMOS ACESSO DE OUTRA FORMA. DESDE O INÍCIO, SEU VALOR PARA DETECÇÃO DE FRAUDES EM PEDIDOS E TRANSAÇÕES FICOU EVIDENTE."

James Coveney, gerente da área de fraudes e crédito da Cashplus

Movimento na sofisticada campanha de roubo de identidades

"Concluímos que os invasores não queriam realmente contas de cartão. Só queriam usar o serviço KYC para validar um conjunto de dados. Se aprovássemos os pedidos, eles saberiam que tinham uma combinação correta de nome, data de nascimento, endereço e outras informações pessoais. Foi um exercício de limpeza", explica James. E que sairia bem caro. Se James e sua equipe não tivessem bloqueado os pedidos, a Cashplus teria recebido uma cara fatura de seu provedor de serviços KYC. Considerando o valor £2 por transação, o ataque teria custado mais de £19.000.

Ainda mais preocupante, essas contas de cartão poderiam ser usadas em fraudes comuns no Reino Unido.

Se contas fraudulentas forem abertas com sucesso, poderão ser usadas para induzir vítimas a transferir fundos para elas mesmas.

Isso, provavelmente, levaria a reclamações de consumidores contra a Cashplus, além de chamar a atenção dos órgãos reguladores. Impedir a aprovação de solicitações fraudulentas foi uma grande conquista para a Cashplus, seus clientes e o público em geral.

Reconhecimento de dispositivos reforça a defesa bem-sucedida da Cashplus

O tipo de dispositivo usado para fazer pedidos fraudulentos apresentou uma pista importante. A tecnologia de reconhecimento de dispositivos TruValidate da TransUnion usa milhares de permutações de atributos para identificar todos os dispositivos visitantes instantaneamente e continuar a reconhecê-los ao longo do tempo, incluindo aqueles provenientes de VPNs, proxy e termos de referência.

"Pela natureza complexa do ataque e a velocidade com que ocorreu, presumo que tenha sido realizado por mais de uma pessoa. Embora tenham mudado a abordagem e as informações pessoais, não tinham controle suficiente sobre os scripts para modificar o tipo de dispositivo. Esse foi o único elemento permanente que conseguimos rastrear durante todo o evento. Os dados do TruValidate possuem o tipo de dispositivo; então, não tivemos nenhum problema com isso", reflete James.

Essa foi a categoria de caso de uso que originalmente convenceu a Cashplus a escolher a TransUnion em detrimento de outros fornecedores. "Depois de analisarmos o mercado em busca de um parceiro para reconhecimento de dispositivos, decidimos adotar a solução da TransUnion devido à variedade de benefícios oferecidos em relação às demais. Queríamos algo que não apenas fornecesse o ID dos dispositivos, mas que também nos permitisse utilizar novos dados sobre os aparelhos que nossos clientes estavam usando e criar regras com base nessas informações", destaca Paul Schooley, diretor operacional da Cashplus.

“OS INVASORES ALTERARAM TODOS OS DETALHES NOS PEDIDOS, MAS O TIPO DE DISPOSITIVO PERMANECEU SEMPRE O MESMO DURANTE O ATAQUE. ISSO NOS PERMITIU IDENTIFICAR AS SOLICITAÇÕES COM MUITO FACILIDADE.”

James Coveney, gerente da área de fraudes e crédito da Cashplus

Depois que James e sua equipe confirmaram que as solicitações eram fraudulentas, ele reportou as evidências de fraude junto ao Consórcio Global de Prevenção à Fraude da TransUnion.

Ao confirmar fraudes envolvendo dispositivos, usuários da solução podem inserir as evidências específicas na base de dados da empresa.

“Garantimos que apenas evidências de fraude confirmadas serão agregadas à nossa base de dados. Não é do interesse de ninguém - nosso, de outros usuários nem dos algoritmos da solução - agir de forma diferente. Ao manter a alta qualidade das evidências, podemos impedir que dispositivos mal-intencionados voltem a prejudicar clientes honestos”, destaca James.

Acesse **https://www.transunion.com.br/industry/fintech** para saber mais sobre as soluções da TransUnion para Instituições Financeiras.para Fintechs.

Para a Cashplus, a solução TransUnion vai além do reconhecimento de dispositivos

O algoritmo da Cashplus tinha uma boa taxa de captura antes de começar a extrair dados do TruValidate. Depois que o reconstruiu para utilizar os dados da solução, o gerente da Cashplus notou que algumas fontes de dados haviam tornado mais valiosos os indicadores de risco, como a idade dos solicitantes, alguns de seus scores e a presença de um proxy, por exemplo.

“Não éramos capazes de identificar esses elementos sem o uso da solução TruValidate. Atualmente, eles são muito úteis. Usamos nosso algoritmo para solicitações como ponto de partida a fim de rastrear os riscos de cada cliente ao longo de seu ciclo de vida conosco. Mesmo quando aceitamos alguns pedidos, a conta associada agora pode fazer parte de uma categoria de risco mais alta do que seria anteriormente, por conta do uso de nossos algoritmos internos combinados com os dados da solução. Isso nos ajuda a detectar e bloquear ações fraudulentas com mais rapidez”, conclui James.

