BOARDROOM
INSIDER COMMUNITY

Proteção da marca e da receita:

redução de bots e violações em toda a jornada do cliente

RETAIL GAZETTE

EM COLABORAÇÃO COM Akamai

Prefácio

Parece que os scrapers viraram um grande problema nos últimos tempos? Você não está imaginando coisas. Após a COVID, os bots de scraping direcionados aos varejistas ficaram mais evasivos — *e sofisticados* — à medida que coletam dados para explorar e monetizar às custas da sua marca.

Mas muitos líderes desconhecem ou subestimam os impactos prejudiciais que os bots de scraping podem ter sobre o desempenho de websites, a segurança de dados e a receita de empresas. Embora os bots de scraping de SEO possam ser benéficos para impulsionar as classificações de pesquisa e a visibilidade, os bots de scraping com intenções mais maliciosas estão sendo implantados para subcotar seus preços, fazer scalping de estoques limitados e criar websites falsificados com o objetivo de roubar informações de clientes. É por isso que é necessário haver mais conscientização e colaboração entre equipes digitais, de marketing, fraude e segurança para proteger não apenas as marcas, mas também os resultados.

Este relatório explica por que a remoção de scrapers de seu website terá diversos impactos positivos para sua organização varejista. Não há como se proteger daquilo que não se pode ver. Sem os scrapers, você terá condições melhores de maximizar seu potencial de receita e otimizar a jornada do cliente até a compra.

Susan McReynolds
Estrategista global do setor comercial na Akamai

Introdução

Os ataques de bots direcionados aos varejistas estão aumentando. As campanhas de phishing direcionadas aos varejistas estão seguindo o mesmo caminho. Coletivamente, as fraudes relacionadas a scraping, fidelidade e cartões de pagamento tiveram um aumento de mais de 700% no segundo semestre de 2023. Sessenta por cento de empresas de comércio eletrônico e 53% de varejistas sofreram um grande aumento nos níveis gerais de fraude. Os canais digitais representaram 52% das perdas gerais relacionadas a fraudes na região EMEA (Europa, Oriente Médio e África), superando as fraudes offline pela primeira vez devido ao anonimato das transações digitais.

O resultado? No ano passado, as perdas por atividade fraudulenta no varejo na região EMEA aumentaram de forma geral, totalizando £ 11,3 bilhões no Reino Unido e € 15 bilhões na Espanha. Noventa e quatro por cento das lojas online na Alemanha foram afetadas por fraude, sendo que 20% delas sofreram perdas de mais de € 100.000.

Isso não é apenas um problema de segurança, mas um desafio de TI para diretores de tecnologia e diretores de informação. É um problema de otimização dos negócios. Para líderes de marca e marketing de varejo em particular, as violações online podem distorcer o tráfego de dados de produtos, de websites e de engajamento, impactando estratégias e orçamentos, bem como a reputação e a confiança conquistadas a duras penas. E o impacto no crescimento pode ser destruidor.

É um desafio crítico para os negócios, com o mesmo objetivo final de melhorar a jornada do cliente e aumentar sua fidelidade. Nesta nova era de fraudes online, as equipes devem trabalhar de forma coletiva e multifuncional para lidar com essa situação.

Como Susan McReynolds, estrategista global do setor comercial na Akamai, afirma, ***"abordar e proteger a jornada do cliente, assim como proteger o lucro, a marca e a receita, exige que todos compreendam o impacto durante todo o ciclo de vida dos pedidos".***

Este relatório descreve:

- Como a pandemia mudou a natureza das ameaças digitais no varejo
- Por que os varejistas devem agir agora
- Tendências de fraude atuais e emergentes
- Seu impacto sobre a marca e a receita
- Como enfrentar esses desafios

Seção 1: como os bots mudaram e por que isso é importante

Durante a pandemia de COVID-19, o aumento da dependência de plataformas digitais (tanto do ponto de vista comercial quanto do consumidor) levou a uma série de novas vulnerabilidades, remodelando fundamentalmente o cenário de fraude no varejo. Como? Os invasores agem pensando no dinheiro. E durante a pandemia, o dinheiro ficou ainda mais concentrado no mundo virtual.

A demanda sem precedentes por determinados produtos como papel higiênico, desinfetantes, fórmulas infantis e equipamentos para exercícios em casa criou oportunidades lucrativas para os operadores de bots explorarem essas condições. Os bots de scraping, por exemplo, acumulavam itens de alta demanda apenas para revendê-los a preços inflacionados, lucrando a partir da escassez e da alta demanda.

Até então, os bots de scraping não estavam causando danos generalizados e significativos e eram bem perceptíveis, o que facilitava combatê-los através de ferramentas de segurança tradicionais. Mas como seu uso era a primeira etapa em um ataque de acúmulo de estoque, e esse acúmulo era muito lucrativo, os operadores de bots decidiram investir recursos significativos para deixar os scrapers mais evasivos.

Ao mesmo tempo, os avanços no machine learning e na IA criaram as condições ideais para os invasores atingirem sua meta. Essa situação também aumentou a capacidade de iniciar vários ataques de uma só vez, usando técnicas sofisticadas de evasão, como endereços IP e proxies rotativos, para driblar os sistemas tradicionais de detecção de bots. **Como Richard Meeus, diretor de tecnologia e estratégia de segurança para a EMEA na Akamai, destaca, *"os bots estão ficando cada vez mais inteligentes. Eles conseguem imitar um ser humano com exatidão e se movimentar sem que ninguém perceba, dificultando a detecção e o combate. Eles também estão surgindo em volumes gigantescos, vindos de milhares de locais diferentes. Nenhum varejista está imune".***

O aumento astronômico das transações online causado pela pandemia (do total das vendas de varejo, a cota correspondente às vendas globais de varejo online cresceu, em média, de 16% para 19% em 2020) também gerou um aumento nas formas mais diretas de fraude, como ATO (apropriação indevida de contas) e ataques de phishing projetados para roubar informações confidenciais. Os varejistas enfrentavam desafios em distinguir entre interações legítimas com clientes e atividades mal-intencionadas de bots, e os agentes malignos exploravam essas fraquezas na pilha de tecnologia de varejo.

Infelizmente, essas suscetibilidades perduram. Os varejistas estão tendo dificuldades para acompanhar a evolução das fraudes e das violações digitais, que está ocorrendo mais rápido que nunca. E com o crescimento do comércio eletrônico global — aproximadamente 22% das vendas globais de varejo em 2024, com estimativa de crescimento a 27% até 2026 —, recai sobre os varejistas o ônus de proteger a quantidade crescente de clientes legítimos que compram online.

Seção 2: como as atividades mal-intencionadas reduzem a receita do varejo e desgastam a confiança do consumidor

O impacto de atividades mal-intencionadas nas empresas de varejo afeta os resultados de maneira central. Um estudo recente descobriu que os comerciantes incorrem em um **custo médio de US$ 3 para cada US$ 1 de fraude**. Os últimos números de 2023 indicam que o custo total da fraude de comércio eletrônico **excede globalmente US$ 48 bilhões**, em comparação com **US$ 41 bilhões em 2022**. As perdas cumulativas por fraude de pagamento online em todo o mundo aumentarão para mais de **US$ 343 bilhões**. Colocando em perspectiva, é mais de três vezes a receita líquida da Apple em 2023.

E esse é apenas o impacto financeiro óbvio, pois ainda há um valor não contabilizado (e, talvez, substancialmente mais caro) de se perder a vantagem competitiva, desgastando o valor, a fidelidade e a confiança na marca. Então, como e onde essa situação se manifesta nos negócios?

O papel do scraping no comprometimento das estratégias de precificação e da exclusividade

O scraping, a prática de extrair dados de websites usando bots automatizados, representa uma ameaça significativa para as marcas, estratégias de preços e exclusividade de produtos dos varejistas. E muitas organizações de varejo nem sabem que têm um problema com scraping, ou, pior ainda, não percebem o verdadeiro impacto que esse tipo de atividade tem sobre os negócios.

Aqui estão seis maneiras como o scraping pode prejudicar seus negócios:

1. Monitoramento e subcotação de preços

Os concorrentes podem usar bots de scraping para monitorar continuamente as informações de preços de um varejista. Com esses dados, eles conseguem subcotar os preços do varejista, o que dificulta a manutenção de uma vantagem competitiva ou a implementação eficaz de estratégias dinâmicas de precificação.

2. Desvantagem competitiva

Aprofundando-se nesse ponto, o scraping de dados de preços, produtos e estoque permite que os concorrentes obtenham insights valiosos sobre as estratégias de um varejista, permitindo que ajustem suas táticas de acordo e obtenham uma vantagem injusta. O campo não está mais nivelado.

3. Perda de exclusividade e de valor da marca

Sabe todo o trabalho que sua equipe de marketing teve para criar imagens e descrições de produtos? Os bots de scraping podem extraí-los, além de outros conteúdos patenteados, do website de um varejista. Esse conteúdo roubado pode ser usado para criar listagens falsificadas ou não autorizadas em marketplaces de terceiros ou até mesmo em websites forjados, prejudicando a exclusividade e o valor da marca.

Em um nível maior, trata-se de um problema de apropriação indevida de marcas. Alguns revendedores não são mal-intencionados, mas muitos estão criando essas páginas apenas para roubar informações de cartão de crédito. E seu consumidor não sabe a diferença.

4. Acúmulo de estoque

Os bots podem capturar dados de estoque em tempo real e burlar os limites de compra ou sistemas de fila, obtendo uma vantagem injusta em relação a clientes humanos; como mencionado anteriormente, isso permite que revendedores ou scalpers acumulem itens limitados ou que estejam na moda, como PlayStations, produtos de marcas de beleza ou sapatos em lançamento exclusivo, impedindo que clientes legítimos os comprem. Mesmo que os clientes possam comprá-los, muitos desses revendedores aumentarão o preço em três vezes ou mais, causando a insatisfação de clientes fiéis.

5. Níveis de estoque imprecisos

Os bots que acumulam ou compram grandes quantidades de produtos podem esgotar rapidamente os níveis de estoque, levando a itens em falta (e clientes decepcionados). Isso tem um efeito negativo adicional na previsão de vendas.

6. Métricas de marketing distorcidas

Esses bots agem como seres humanos, e as análises realizadas por você os refletirão dessa forma, deixando os dados de marketing distorcidos. Para um dos clientes da Akamai, 90% de seu tráfego acabou sendo de bots, o que teve um grande impacto em suas campanhas de marketing e custos de nuvem.

Christine Ross, diretora de marketing de produtos da Akamai, descreve a situação: "Os clientes nos dizem: 'Este produto é selecionado no meu website o tempo todo. Ele deve ser bem popular mesmo', mas na verdade são bots que o selecionam, não pessoas. Por isso, eles adquirem mais quantidades de um produto específico porque o website apontou que ele estava em alta, mas, na verdade, as pessoas não estavam comprando esse item nem acessando aquela página. Isso afeta as principais decisões de otimização de estoque e website. E, às vezes, se você não desconsiderar os dados relativos a bots, você otimizará para os bots e não para os consumidores, o que poderá erradicar o ROI de marketing e dificultar o crescimento dos negócios".

Redução do desempenho de websites e suas repercussões no engajamento de usuários

Outra área problemática é o desempenho de websites, a janela de um varejista para o mundo. Os bots que executam scraping ou acúmulo de estoque podem sobrecarregar a infraestrutura do website de um varejista, levando a lentidão no tempo de carregamento, aumento dos custos de servidor e até mesmo interrupções no funcionamento do website. Essa degradação no desempenho afeta diretamente o engajamento do usuário, pois os clientes que enfrentam lentidão no carregamento de páginas ou tempo de inatividade provavelmente abandonarão o website e optarão pela concorrência.

Considerando o fato de que a média de visualizações de página por sessão de compra se estendeu para além de 20 páginas em 2023, destacando a necessidade de mais páginas e conteúdo para conversão, um website de alto desempenho se mostra ainda mais essencial. A frustração dos usuários com os websites de varejo é um problema real e constante, afetando 40% das experiências dos compradores. Isso se correlaciona diretamente com a conversão e custa aos varejistas quase US$ 0,60 por visita em desperdício de gastos.

Uma experiência de usuário ruim também é inimiga da retenção. Os clientes que retornam convertem quatro vezes mais que os novos e têm menos probabilidade de chegar a partir de canais pagos. Se você for líder de marketing e estiver fazendo malabarismos com um orçamento apertado, esse será um ponto importante a ser observado.

Contas comprometidas e os custos financeiros e de reputação associados

Ataques de preenchimento de credencial e campanhas de phishing orientados por bots podem levar ao comprometimento de contas de clientes, o que é particularmente prejudicial. Essas credenciais roubadas podem ser usadas para apropriação indevida de contas, roubo de identidade ou até mesmo violações de dados, afetando as finanças e a segurança dos clientes. E a culpa cai diretamente no seu colo.

Do ponto de vista do varejista, o acesso não autorizado a contas pode levar imediatamente a pedidos e estornos fraudulentos, roubo de pontos de fidelidade, violações de cupons/promoções, revenda de contas e ataques de validação de CVV, citando apenas alguns. Os extensos ataques de apropriação indevida de contas podem incluir a substituição de ativos para clientes, possíveis multas, redução da confiança na marca, aumento dos custos de investigação de fraude e burnout nas equipes de fraude, segurança e marketing.

Com relação às violações de dados, os custos financeiros para lidar com as correções incluem:

Custos operacionais maiores

(por exemplo, segurança, conformidade ou mesmo, como na loja Neiman Marcus em 2021, com a criação de um call center dedicado a reclamações de clientes sobre como eles foram afetados).

Serviços de reembolso e monitoramento de crédito

para clientes afetados (um exemplo disso inclui a Hudson's Bay em 2018, que ofereceu serviços de proteção de identidade para clientes expostos).

Custos e acordos judiciais

Após uma violação de informações de cartão de pagamento em 2013, a gigante varejista Target precisou lidar com uma série de ações judiciais, totalizando quase US$ 300 milhões. O impacto no crescimento foi grave: os lucros da Target caíram quase 50% no 4º trimestre daquele ano em comparação com o ano anterior, e o preço de suas ações caiu 9% nos dois meses subsequentes.

Investigações e multas regulatórias

No caso da Target, o Departamento de Justiça dos EUA abriu uma investigação. Quando a Dixons Carphone teve as informações de 14 milhões de clientes comprometidas em 2018, o Information Commissioner's Office (ICO) a multou no valor máximo de £ 500.000.

Os custos à reputação causados por contas comprometidas e vazamentos também afetam o crescimento geral. Cinquenta e quatro por cento dos clientes dizem que trocariam para uma marca diferente se a que usavam sofresse uma violação de dados. Para empresas de capital aberto, elas sofrem uma perda média de 3,5% no preço de suas ações após uma violação. No caso da Dixons Carphone, o declínio dos lucros levou ao encerramento de 100 lojas Carphone Warehouse dentro de um ano e da totalidade da marca Carphone Warehouse em 2020.

As contas comprometidas são um fator significativo na percepção, confiança e lealdade do cliente, que estão no centro dos objetivos de cada líder de marca e marketing. Por exemplo, a percepção do consumidor da Target pré-violação ficou em 20,7 na classificação Brand Index Buzz, caindo para um nível baixo de 9,4 no ano seguinte. Cinco anos mais tarde, o número chegou a 17,3, descrevendo a dificuldade que enfrentaram para recuperar sua reputação entre os consumidores. No ambiente conectado e saturado de redes sociais de hoje, a percepção da marca pode ser criada ou destruída em minutos.

A mudança no comportamento dos consumidores, juntamente com a crise do custo de vida, também virou a fidelidade de cabeça para baixo. A confiança, uma porta de entrada para a fidelidade, é a chave para conquistar a próxima geração de consumidores e promover o crescimento sustentável dos negócios. Os millenials e a geração Z têm os níveis mais baixos de confiança de marca, talvez atribuídos ao fato de que aproximadamente 20% deles tiveram seus dados comprometidos (em comparação com 2% da geração X e 10% dos baby boomers).

Portanto, essa construção de confiança requer experiências rápidas, sem atritos e sem fraude. Os compradores estão dispostos a pagar 46% mais para um varejista em quem confiam. O fator mais alto para alcançar essa confiança? Um processo seguro de finalização de compra e proteção de dados pessoais. Um estudo global de 2023 descreve que quase 90% dos consumidores afirmam que isso é vital para os varejistas alcançarem esse objetivo. Uma reputação forte da marca também figurou na lista principal, com 76%.

Conclusão: combater os bots e as violações por meio do alinhamento organizacional

Talvez pareça um desafio gigantesco o enfrentamento dessas tecnologias maliciosas e seu crescimento desenfreado, mas não precisa ser assim. A boa notícia é que existem maneiras eficazes de manter sua marca sob controle e melhorar a jornada do seu cliente. Mas por onde começar?

Estratégias para proteger sua marca e seus resultados

Não surpreende que equipes diferentes estejam geralmente concentradas na proteção de diferentes resultados: o setor de segurança protege os dados, o de marketing protege a receita, o de TI protege contra interrupções, o de CX protege o caminho do cliente até a compra. Mas essas equipes têm vários desafios a enfrentar:

- *Elas estão se comunicando e em sintonia quanto aos resultados e metas comerciais compartilhados?*
- *Elas conseguem responder à pergunta: "As partes interessadas estão alinhadas com os requisitos técnicos e as ferramentas para proteger os dados do cliente, a marca e a receita?"*

Na maioria das vezes, descobrimos que a resposta é não, mas isso é fundamental. Outras perguntas importantes que essas equipes precisam responder coletivamente incluem:

- *Quais são os resultados que estamos tentando alcançar (p. ex., proteger a receita, os dados do cliente, o caminho para a compra, fraude)?*
- *Precisamos de uma solução ou de várias soluções para resolver vários desafios e casos de uso das partes interessadas?*
- *Existe uma desconexão entre quem está comprando a solução e quem está realmente usando-a?*
- *O que é o sucesso? Temos KPIs claramente definidos?*
- *O que estamos dispostos a tolerar/quais compensações devem ser feitas para equilibrar a segurança com a necessidade de otimizar o caminho para a compra?*
- *Estamos protegendo todo o nosso patrimônio (website, app móvel, APIs e infraestrutura)?*
- *Como lidamos com nossos objetivos, empecilhos e o limite impreciso entre esses dois aspectos?*

Cada equipe precisa entender esses pontos e ter uma meta compartilhada que impulsione o alinhamento e a ação para obter resultados ideais para a empresa.

A fraude no varejo está avançando em um ritmo muito acelerado e tendo um impacto generalizado nos varejistas. Como descrevemos, as perdas vão além daquelas vistas com facilidade em uma lista de multas, acordos ou honorários advocatícios. Atingem em cheio o objetivo final do varejista de gerar receita por meio da fidelidade da marca e do cliente. A marca e a fidelidade dependem da confiança e da experiência do cliente, fatores reduzidos em um piscar de olhos por meio de atividades fraudulentas.

O aumento dos ataques, aliado a um cenário de compras complexo e à constante escalada das vendas online, significa que é mais vital do que nunca que os varejistas priorizem e invistam em medidas de segurança avançadas para proteger sua marca e seus clientes. Significa que as unidades de negócios devem trabalhar juntas para entender e compartilhar o impacto de ataques mal-intencionados, já que não são mais o domínio da segurança e das equipes de TI sozinhas.

Se precisar de apoio, entre em contato com a equipe da Akamai ou saiba mais sobre soluções de varejo, turismo e hotelaria. A Akamai tem ajudado varejistas e marcas globais, como a Lufthansa, o Wagner eCommerce Group, a Panasonic e a TOUS a proporcionarem experiências online seguras e envolventes há mais de 25 anos.

Sobre a Akamai

A Akamai potencializa e protege a vida online. As principais empresas do mundo escolhem a Akamai para criar, entregar e proteger suas experiências digitais, ajudando bilhões de pessoas a viver, trabalhar e se divertir todos os dias. A Akamai Connected Cloud, uma plataforma de nuvem e edge amplamente distribuída, aproxima os aplicativos e as experiências dos usuários e afasta as ameaças. Saiba mais sobre as soluções de computação em nuvem, segurança e entrega de conteúdo da Akamai em akamai.com e akamai.com/blog, ou siga a Akamai Technologies no X, antigo Twitter, e LinkedIn.

Este documento foi desenvolvido em conjunto com a Retail Gazette, a maior publicação de varejo B2B do Reino Unido.

Visite **www.retailgazette.co.uk** para juntar-se a 300.000 outros usuários mensais para ter acesso gratuito às últimas notícias, entrevistas, análises, relatórios detalhados e white papers.

Publicado em 07/24