BOARDROOM
INSIDER COMMUNITY

Protection de la marque et de ses revenus :

réduire les bots et les abus tout au long du parcours client

RETAIL GAZETTE

EN COLLABORATION AVEC Akamai

Avant-propos

Vous avez l'impression que les extracteurs sont devenus un problème de taille ces derniers temps ? Ce n'est pas le fruit de votre imagination. Après la pandémie de COVID, les bots d'extraction qui ciblent les détaillants sont devenus plus évasifs (*et plus sophistiqués*), car ils récoltent des données pour les exploiter et les monétiser aux dépens de votre marque.

Mais de nombreux dirigeants ignorent ou sous-estiment les effets néfastes que les bots d'extraction peuvent avoir sur les performances des sites Web, la sécurité des données et les revenus de l'entreprise. Alors que les bots d'extraction SEO peuvent être bénéfiques pour améliorer le classement des recherches et la détectabilité, des bots d'extraction avec des intentions plus néfastes sont déployés pour réduire vos prix, s'approprier les stocks limités et créer des sites de contrefaçon visant à voler les informations des clients. C'est pourquoi une plus grande sensibilisation (et une collaboration entre les équipes chargées du digital, du marketing, de la fraude et de la sécurité) est nécessaire pour protéger non seulement la marque, mais aussi les résultats.

Ce rapport explique pourquoi la suppression des bots d'extraction de votre site Web aura un impact positif sur de nombreuses facettes de votre organisation de commerce de détail. Vous ne pouvez pas vous protéger contre ce que vous ne pouvez pas voir. Une fois les bots d'extraction supprimés, vous pourrez mieux maximiser votre potentiel de revenus et optimiser le parcours d'achat de vos clients.

Susan McReynolds
Global Industry Strategist, Commerce, Akamai

Introduction

Les attaques par bots ciblant les détaillants se multiplient. Les campagnes d'hameçonnage ciblant les détaillants sont également en hausse. Ensemble, les fraudes à l'extraction, à la fidélisation et aux cartes de paiement ont connu une hausse de plus de 700 % au cours du second semestre 2023. 60 % des commerçants en ligne et 53 % des détaillants ont connu une hausse des niveaux de fraude globaux. Les canaux digitaux représentaient 52 % des pertes totales liées à la fraude dans la région EMEA, dépassant pour la première fois la fraude physique en raison de l'anonymat des transactions digitales.

Le résultat ? L'année dernière, les pertes liées aux activités frauduleuses de vente au détail dans la zone EMEA ont augmenté de manière générale, atteignant 11,3 milliards de livres sterling au Royaume-Uni et 15 milliards d'euros en Espagne. Quatre-vingt-quatorze pour cent des boutiques en ligne en Allemagne ont été touchées par la fraude, et 20 % d'entre elles ont subi des pertes de plus de 100 000 €.

Il ne s'agit pas seulement d'un problème de sécurité (un défi informatique à résoudre pour les directeurs techniques et les directeurs des systèmes d'information). Il s'agit d'un problème d'optimisation commerciale. Pour les responsables des marques et du marketing du commerce de détail en particulier, les abus en ligne peuvent fausser les données sur les produits, le site Web et le trafic d'engagement, ce qui a un impact sur la stratégie et les budgets, ainsi que sur la réputation et la confiance durement gagnées. Et l'impact sur la croissance peut être dévastateur.

Il s'agit d'un défi stratégique pour l'entreprise, dont l'objectif final est le même : améliorer le parcours du client et le fidéliser. Dans cette nouvelle ère de fraude en ligne, les équipes doivent briser les silos et travailler de manière transversale pour y faire face.

Comme l'affirme Susan McReynolds, Global Industry Strategist, Commerce, Akamai, *« Pour s'attaquer au parcours du client et le protéger, pour protéger vos profits, votre marque et vos revenus, il faut que tout le monde comprenne l'impact sur l'ensemble du cycle de vie de la commande. »*

Ce rapport décrit les points suivants :

- Comment la pandémie a changé la nature des menaces digitales dans le commerce de détail
- Pourquoi les détaillants doivent agir maintenant
- Les tendances actuelles et émergentes en matière de fraude
- Leur impact sur la marque et le chiffre d'affaires
- Comment relever ces défis

Section 1 : Comment les bots ont changé, et pourquoi c'est important

Au cours de la pandémie de COVID-19, la dépendance accrue à l'égard des plateformes digitales (tant du point de vue des entreprises que des consommateurs) a engendré une multitude de nouvelles vulnérabilités, qui ont fondamentalement remodelé le paysage de la fraude dans le secteur du commerce de détail. Mais comment ? Les attaquants suivent l'argent. Et pendant la pandémie, cet argent s'est déplacé plus que jamais en ligne.

La demande sans précédent de certains produits tels que le papier hygiénique, les désinfectants, le lait maternisé et le matériel d'entraînement à domicile a créé des opportunités lucratives pour les opérateurs de bots qui ont exploité ces conditions. Les bots d'extraction, par exemple, ont accumulé des articles très demandés pour les revendre à des prix élevés, profitant ainsi de la pénurie et de la forte demande des consommateurs.

Jusqu'à ce moment-là, les bots d'extraction ne causaient pas de dommages étendus importants et étaient assez perceptibles. Il était donc plus facile de les combattre à l'aide d'outils de sécurité traditionnels. Mais comme ils constituaient la première étape d'une attaque d'accaparement des stocks, et que cet accaparement était extrêmement rentable, les opérateurs de bots ont décidé d'investir dans des ressources importantes pour rendre les extracteurs plus évasifs.

Dans le même temps, les progrès de l'apprentissage automatique et de l'IA ont créé des conditions idéales pour permettre aux attaquants d'atteindre leur objectif. Ils ont également pu renforcer leur capacité à lancer plusieurs attaques à la fois, en utilisant des techniques d'évasion sophistiquées, telles que la rotation des adresses IP et des proxys, pour contourner les systèmes traditionnels de détection des bots. **Comme l'a souligné Richard Meeus, Director of Security Technology and Strategy EMEA chez Akamai, *« Les bots sont de plus en plus intelligents. Ils peuvent imiter un être humain à la perfection et entrer et sortir sans même que vous ne les voyiez, ce qui les rend plus difficiles à détecter et à combattre. Ils arrivent également en très grand nombre, en provenance de milliers d'endroits différents. Aucun détaillant n'est à l'abri. »***

L'augmentation astronomique des transactions en ligne provoquée par la pandémie (la part des ventes en ligne dans le total des ventes au détail est passée en moyenne de 16 % à 19 % en 2020) a également entraîné une augmentation des formes de fraude plus directes, telles que les attaques par prise de contrôle de compte (ATO) et par hameçonnage, destinées à voler des informations sensibles. Les détaillants ont eu du mal à faire la distinction entre les interactions légitimes avec les clients et les activités malveillantes des bots. Les acteurs malveillants ont alors exploité ces faiblesses dans la pile technologique du commerce de détail.

Malheureusement, ces vulnérabilités demeurent. Les détaillants s'efforcent de suivre le rythme de l'évolution de la fraude et des abus digitaux, qui font effet boule de neige plus rapidement que jamais. Et avec la croissance du commerce électronique mondial (environ 22 % des ventes au détail mondiales en 2024, qui devraient atteindre 27 % en 2026), il incombe aux détaillants de protéger le nombre croissant de clients légitimes qui font leurs achats en ligne.

Section 2 : Comment les activités malveillantes réduisent les revenus du commerce de détail et érodent la confiance des consommateurs

L'impact des activités malveillantes sur les détaillants se répercute fondamentalement sur les résultats. Une étude récente a révélé que les commerçants subissent un coût moyen **de 3 $ pour chaque dollar de fraude**. Les derniers chiffres de 2023 indiquent que le coût total de la fraude au commerce électronique **dépasse 48 milliards de dollars à l'échelle mondiale**, contre **41 milliards de dollars en 2022**. Les pertes cumulées dues à la fraude sur les paiements en ligne s'élèveront à plus de **343 milliards de dollars**. Pour mettre les choses en perspective, cela représente plus de trois fois le revenu net d'Apple en 2023.

Et il ne s'agit là que de l'impact financier évident : il y a toujours une valeur non prise en compte (et sans doute beaucoup plus coûteuse) à la perte d'un avantage concurrentiel, se traduisant par une certaine érosion de l'image de marque, de la fidélité et la confiance envers la marque. Comment et où cela se manifeste-t-il dans l'entreprise ?

Le rôle de l'extraction dans l'affaiblissement des stratégies de prix et de l'exclusivité des produits

L'extraction, qui consiste à extraire des données de sites Web à l'aide de bots, représente une menace importante pour les marques, les stratégies de prix et l'exclusivité des produits des détaillants. De nombreuses organisations de vente au détail ne savent même pas qu'elles ont un problème d'extraction ou, pire encore, ne réalisent pas l'impact réel de ce type d'activité sur leur propre activité.

Voici six façons dont l'extraction peut nuire à votre entreprise :

1. Surveillance des prix et sous-cotation

Les concurrents peuvent utiliser des bots d'extraction pour surveiller en permanence les informations sur les prix d'un détaillant. Grâce à ces données, ils peuvent pratiquer des prix inférieurs à ceux du détaillant, ce qui rend difficile le maintien d'un avantage concurrentiel ou la mise en œuvre efficace de stratégies de tarification dynamique.

2. Désavantage concurrentiel

En approfondissant ce point, l'extraction de données sur les prix, les produits et les stocks permet aux concurrents d'obtenir des informations précieuses sur les stratégies d'un détaillant, ce qui leur donne la possibilité d'ajuster leurs propres tactiques en conséquence et d'obtenir un avantage déloyal. Les règles du jeu ne sont plus les mêmes pour tous.

3. Perte d'exclusivité et de valeur de la marque

Vous avez conscience de tous les efforts que votre équipe marketing a déployés pour créer des images et des descriptions de produits ? Les bots d'extraction peuvent les extraire, ainsi que d'autres contenus exclusifs, du site Web d'un détaillant. Ce contenu volé peut ensuite être utilisé pour créer des listes contrefaites ou non autorisées sur des places de marché tierces ou même sur des sites Web similaires, ce qui porte atteinte à l'exclusivité et à la valeur de la marque.

À plus grande échelle, il s'agit d'un problème d'usurpation d'identité de marque. Certains revendeurs ne sont pas malveillants, mais beaucoup d'entre eux le sont et créent ces pages dans le seul but de voler des informations sur les cartes de crédit. Et le consommateur ne fait pas la différence.

4. Accaparement de stocks

Les bots peuvent récupérer des données d'inventaire en temps réel et contourner les limites d'achat ou les systèmes de file d'attente, ce qui leur donne un avantage injuste sur les clients humains. Comme nous l'avons déjà mentionné, cela permet aux revendeurs ou aux vendeurs à la sauvette d'accumuler des éditions limitées ou des articles très demandés, tels que des PlayStation, des marques de produits de beauté ou des chaussures, laissant les clients légitimes dans l'impossibilité d'effectuer des achats. Même s'ils y parviennent, nombre de ces revendeurs multiplient le prix par trois ou plus, ce qui suscite la colère des clients fidèles.

5. Niveaux de stock inexacts

Les bots qui accumulent ou achètent de grandes quantités de produits peuvent rapidement épuiser les niveaux de stock, ce qui entraîne des ruptures de stock (et la déception des clients). Cela a également un effet négatif sur les prévisions de ventes.

6. Des mesures marketing faussées

Ces bots se comportent comme des humains et vos analyses les reflètent comme tels, ce qui fausse vos données marketing. Le trafic de l'un des clients d'Akamai était constitué à 90 % de bots, ce qui a eu un impact majeur sur ses campagnes marketing et ses coûts liés au cloud.

Comme l'explique Christine Ross, Marketing Director, Akamai : « Les clients nous ont dit : "Ce produit est constamment affiché sur mon site Web. Il doit être très populaire", mais ce sont en fait les bots qui le consultent et non les humains. Ils ont donc acheté davantage d'exemplaires d'un produit particulier parce que le site Web disait qu'il était populaire, mais en fait, les gens ne l'achetaient pas. Personne ne consultait cette page. Cela a un impact sur les décisions importantes en matière d'inventaire et d'optimisation du site Web. Et parfois, si vous n'en tirez pas les données relatives aux bots, vous optimisez pour les bots et non pour les consommateurs. Cela peut réduire le retour sur investissement du marketing et entraver la croissance de l'entreprise. »

Baisse des performances du site et ses répercussions sur l'engagement des utilisateurs

Les performances du site Web, qui est la vitrine du détaillant sur le monde, sont également touchées de plein fouet. Les bots qui effectuent de l'extraction ou de l'accumulation d'inventaire peuvent surcharger l'infrastructure du site Web d'un détaillant, ce qui entraîne des temps de chargement plus lents, une augmentation des coûts de serveur et même des pannes de site. Cette dégradation des performances a un impact direct sur l'engagement des utilisateurs, car les clients confrontés à des pages qui se chargent lentement ou à des temps d'arrêt sont susceptibles d'abandonner le site et de se tourner vers la concurrence.

Étant donné que le nombre moyen de pages vues par session d'achat dépassera 20 pages en 2023, ce qui souligne la nécessité d'augmenter le nombre de pages et le contenu pour la conversion, disposer d'un site Web hautement performant devient d'autant plus crucial. La frustration des utilisateurs à l'égard des sites Web de vente au détail est réelle et répandue, affectant 40 % des expériences d'achat. Cela est directement lié à la conversion, et coûte aux détaillants près de 0,60 $ par visite en dépenses gaspillées.

Une mauvaise expérience utilisateur est également l'ennemi de la fidélisation. Les clients qui reviennent convertissent quatre fois plus que les nouveaux et sont moins susceptibles de provenir des canaux payants. Si vous êtes responsable marketing et que vous devez jongler avec un budget de plus en plus serré, il s'agit là d'un point essentiel.

Comptes compromis et coûts financiers et de réputation associés

Les attaques par « credential stuffing » et les campagnes d'hameçonnage menées par des bots peuvent conduire à la compromission de comptes clients, ce qui est particulièrement préjudiciable. Ces informations d'identification volées peuvent ensuite être utilisées pour la prise de contrôle de comptes, l'usurpation d'identité ou même la violation de données : autant d'éléments qui affectent les finances et la sécurité des clients, et dont la responsabilité vous incombe directement.

Du point de vue du détaillant, l'accès non autorisé à un compte peut immédiatement conduire à des commandes frauduleuses et à des rétrofacturations, au vol de points de fidélité, à l'abus de coupons/promotions, à la revente de comptes et à des attaques de validation CVV, pour n'en nommer que quelques-uns. Les retombées à long terme d'un piratage de compte peuvent inclure le remplacement d'actifs pour les clients, des amendes potentielles, une diminution de la confiance dans la marque, une augmentation des coûts d'investigation sur les fraudes et l'épuisement des équipes chargées de la fraude, de la sécurité et du marketing.

En ce qui concerne les violations de données, les coûts financiers liés à la remédiation sont les suivants :

Augmentation des coûts opérationnels

(par exemple, la sécurité, la conformité ou même, comme pour Neiman Marcus en 2021, la mise en place d'un centre d'appel dédié pour répondre aux plaintes des clients sur la manière dont ils ont été impactés.)

Remboursements et services de contrôle du crédit

pour les clients touchés (par exemple, Hudson Bay a proposé en 2018 des services de protection de l'identité à ses clients victimes d'une violation.)

Frais juridiques et règlements

Après une violation des informations relatives aux cartes de paiement en 2013, le géant du commerce de détail Target a dû régler une série de poursuites, totalisant près de 300 millions de dollars. L'impact sur la croissance de l'entreprise a été grave : les bénéfices de Target ont chuté de près de 50 % au quatrième trimestre de cette année-là par rapport à l'année précédente, et le cours de son action a baissé de 9 % au cours des deux mois qui ont suivi.

Amendes et enquêtes réglementaires

Dans le cas de Target, le ministère de la Justice a lancé une enquête. Lorsque les informations de 14 millions de clients de Dixons Carphone ont été compromises en 2018, l'Information Commissioner's Office a infligé la sanction maximale de 500 000 £.

Les coûts de réputation des comptes compromis et des violations ont également un impact sur la croissance globale. Cinquante-quatre pour cent des clients déclarent qu'ils changeraient de marque si celle qu'ils utilisent subissait une violation de données. Les entreprises cotées en bourse subissent une perte moyenne de 3,5 % sur le cours de leurs actions après une violation. Dans le cas de Dixons Carphone, la baisse des bénéfices a conduit à la fermeture de 100 magasins Carphone Warehouse en l'espace d'un an et à la disparition totale de la marque Carphone Warehouse jusqu'à 2020.

Les comptes compromis sont un facteur important de la perception, de la confiance et de la fidélité des clients, qui sont au cœur des objectifs de toute marque et de tout responsable marketing. Par exemple, la perception des consommateurs de Target avant la violation était de 20,7 sur l'indice Buzz du Brand Index, et a chuté à un minimum de 9,4 l'année suivante. Cinq ans plus tard, ce chiffre s'élevait à 17,3, ce qui montre bien la montagne qu'il a fallu gravir pour retrouver sa position parmi les consommateurs. Dans l'environnement connecté et saturé de médias sociaux d'aujourd'hui, la perception d'une marque peut se faire ou se défaire en quelques minutes.

L'évolution du comportement des consommateurs, conjuguée à la crise du coût de la vie, a également bouleversé leur fidélité. La confiance, porte d'entrée de la fidélité, est essentielle pour gagner la prochaine génération de consommateurs et favoriser une croissance durable des entreprises. Les générations Y et Z sont les personnes qui ont le moins confiance dans les marques, ce qui s'explique peut-être par le fait qu'environ 20 % d'entre elles ont vu leurs données sciemment compromises (contre 2 % pour la génération X et 10 % pour la génération des baby-boomers).

C'est pourquoi l'instauration de la confiance passe par des expériences rapides, sans friction et sans fraude. Les acheteurs sont prêts à payer 46 % de plus auprès d'un détaillant en qui ils ont confiance. Le facteur le plus important pour obtenir cette confiance ? Un processus de paiement sécurisé et la protection des données personnelles. Une étude mondiale de 2023 souligne que près de 90 % des consommateurs déclarent que cela est essentiel pour que les détaillants atteignent cet objectif. Une solide réputation de la marque figure également en tête de liste, avec 76 %.

Conclusion : combattre les bots et les abus par l'alignement organisationnel

Compte tenu de l'ampleur croissante de ces technologies malveillantes, on peut avoir l'impression d'être confronté à un nouveau défi de taille. Pourtant, ce n'est pas une fatalité. La bonne nouvelle, c'est qu'il existe des moyens efficaces de garder le contrôle de votre marque et d'améliorer le parcours de vos clients. Mais par où commencer ?

Stratégies de protection de votre marque et de vos résultats financiers

Il n'est pas surprenant que plusieurs équipes se concentrent généralement sur la protection de différents résultats : la sécurité protège les données, le marketing protège le chiffre d'affaires, l'informatique protège contre les pannes, l'expérience client protège le parcours du client jusqu'à l'achat. Mais ces équipes doivent relever plusieurs défis :

- *Communiquent-elles et sont-elles sur la même longueur d'onde en ce qui concerne les résultats et les objectifs communs de l'entreprise ?*
- *Peuvent-elles répondre à la question suivante : « Les parties prenantes sont-elles d'accord sur les exigences techniques et les outils nécessaires pour protéger les données des clients, la marque et le chiffre d'affaires ? »*

La plupart du temps, la réponse est négative. Mais il s'agit là d'un point essentiel. Voici d'autres questions clés auxquelles ces équipes doivent répondre collectivement :

- *Quels sont les résultats que nous essayons d'atteindre (par exemple, la protection du chiffre d'affaires, des données des clients, du parcours d'achat, contre la fraude) ?*
- *Avons-nous besoin d'une solution ou de plusieurs solutions pour résoudre les différents défis et cas d'utilisation des parties prenantes ?*
- *Existe-t-il un décalage entre ceux qui achètent la solution et ceux qui l'utilisent réellement ?*
- *À quoi ressemble le succès ? Avons-nous des KPI clairement définis ?*
- *Que sommes-nous prêts à tolérer/quels compromis devons-nous faire pour équilibrer la sécurité et la nécessité d'optimiser le parcours d'achat ?*
- *Protégeons-nous l'ensemble de notre patrimoine (site Web, application pour mobile, API et infrastructure) ?*
- *Comment gérer le désiré, le non désiré et la frontière floue entre les deux ?*

Chaque équipe doit comprendre ces points et avoir un objectif commun qui favorise l'alignement et l'action afin d'obtenir des résultats optimaux pour l'entreprise.

La fraude dans le commerce de détail s'accélère à un rythme effréné et a un impact considérable sur les détaillants. Comme nous l'avons souligné, les pertes vont au-delà de celles facilement visibles sur un registre, sous forme d'amendes, de règlements ou de frais juridiques. Elles touchent le cœur de l'objectif ultime des détaillants, qui est de générer des revenus grâce à la marque et à la fidélité des clients. La marque et la fidélité reposent sur la confiance et l'expérience du client, des facteurs diminués en un clin d'œil par des activités frauduleuses.

L'augmentation des abus, associée à un paysage d'achat difficile pour les consommateurs et à l'augmentation constante des ventes en ligne, signifie qu'il est plus vital que jamais pour les détaillants de donner la priorité et d'investir dans des mesures de sécurité avancées afin de protéger leur marque et leurs clients. Cela signifie que les unités commerciales doivent travailler ensemble pour comprendre et partager l'impact des attaques malveillantes, car elles ne sont plus l'apanage des seules équipes de sécurité et d'informatique.

Si vous avez besoin d'assistance, contactez l'équipe Akamai ou découvrez les solutions de commerce de détail, de tourisme et d'hôtellerie. Depuis plus de 25 ans, Akamai aide des détaillants et des marques internationales telles que Lufthansa, Wagner eCommerce Group, Panasonic et TOUS à offrir des expériences en ligne sûres et attrayantes.

À propos d'Akamai

Akamai soutient et protège la vie en ligne. Les entreprises leaders du monde entier choisissent Akamai pour concevoir, diffuser et sécuriser leurs expériences digitales, et aident des milliards de personnes à vivre, travailler et jouer chaque jour. Akamai Connected Cloud, plateforme cloud massivement distribuée en bordure de l'Internet, rapproche les expériences et les applications des utilisateurs tout en éloignant les menaces. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn.

Cet article vous a été présenté conjointement avec Retail Gazette, la plus grande publication B2B de commerce de détail du Royaume-Uni.

Rendez-vous sur **www.retailgazette.co.uk** pour rejoindre les 300 000 autres utilisateurs mensuels et accéder gratuitement aux dernières nouvelles, interviews, analyses, ainsi qu'aux derniers rapports approfondis et livres blancs.

Publication : 07/24