BOARDROOM
INSIDER COMMUNITY

Proteger las marcas y los ingresos:

Reducir los bots y el uso indebido en toda la experiencia del cliente

RETAIL GAZETTE

EN COLABORACIÓN CON Akamai

Prólogo

¿Tiene la sensación de que los scrapers se han convertido en un gran problema últimamente? No se lo está imaginando. Después de la pandemia de COVID, los bots scrapers dirigidos a los retailers se han vuelto más evasivos (*y sofisticados*) cuando recopilan datos para explotarlos y monetizarlos a costa de su marca.

Sin embargo, muchos líderes desconocen, o subestiman, los efectos perjudiciales que pueden tener los bots scrapers en el rendimiento del sitio web, la seguridad de los datos y los ingresos de la empresa. Aunque los bots scrapers de SEO pueden ser beneficiosos para mejorar el posicionamiento en los motores de búsqueda y la capacidad de detección, se están implementando bots scrapers con intenciones más nocivas, como hacer guerra de precios, acaparar inventario y crear sitios falsificados destinados a robar información de los clientes. Por eso es necesario aumentar la concienciación y la colaboración entre los equipos digitales, de marketing, de lucha contra el fraude y de seguridad, no solo para proteger la marca, sino también los resultados netos.

Este informe aclara por qué la eliminación de los scrapers de su sitio web tendrá un impacto positivo en muchas facetas de su organización de retail. No podemos defendernos de lo que no vemos. Con los scrapers fuera de juego, estará mejor preparado para maximizar su potencial de ingresos y optimizar la experiencia de compra de sus clientes.

Susan McReynolds
Estratega del Sector Global en Comercio de Akamai

Introducción

Los ataques de bots dirigidos a los retailers aumentan. Las campañas de phishing dirigidas a los retailers también están aumentando. En conjunto, el fraude relacionado con el scraping, los programas de fidelidad y las tarjetas de pago registró un aumento de más del 700 % en la segunda mitad de 2023. El 60 % de los comerciantes de e-commerce y el 53 % de los retailers experimentaron un aumento en los niveles generales de fraude. Los canales digitales representaron el 52 % de las pérdidas totales por fraude en la región de EMEA, superando por primera vez al fraude físico debido al anonimato de las transacciones digitales.

¿El resultado? El año pasado, las pérdidas por actividades fraudulentas en el sector del retail en EMEA aumentaron de forma generalizada, alcanzando los 11 300 millones de libras en el Reino Unido y los 15 000 millones de euros en España. El 94 % de las tiendas online de Alemania se vieron afectadas por el fraude, y el 20 % de ellas experimentó pérdidas de más de 100 000 €.

No se trata solo de un problema de seguridad, es decir, no se trata de un desafío de TI que los directores de tecnología y los directores de TI deben resolver. Se trata de un problema de optimización empresarial. Para los responsables de marketing y de marcas de retail en concreto, el uso indebido online puede distorsionar los datos de productos y el tráfico del sitio web y de participación de los usuarios, lo que afecta a la estrategia y los presupuestos, así como a la reputación y la confianza que con tanto esfuerzo se han logrado. Y el impacto en el crecimiento puede ser devastador.

Se trata de un desafío esencial para las empresas, con el mismo objetivo final de mejorar la experiencia del cliente y aumentar su fidelidad. En esta nueva era del fraude online, los equipos deben eliminar los silos y trabajar de forma multifuncional para abordarlo.

Tal como afirma Susan McReynolds, estratega del Sector Global en Comercio de Akamai, ***"Abordar y proteger la experiencia del cliente, proteger sus beneficios, y proteger la marca y los ingresos requiere que todos comprendan el impacto que tiene todo el ciclo de vida de ese pedido".***

En este informe se describe:

- Cómo cambió la pandemia la naturaleza de las amenazas digitales en el sector del retail.
- Por qué los retailers deben actuar ahora.
- Tendencias actuales y emergentes del fraude.
- El impacto que tienen en la marca y los ingresos.
- Cómo afrontar estos desafíos.

Sección 1: Cómo han cambiado los bots y por qué es importante

Durante la pandemia de la COVID-19, el aumento de la dependencia de las plataformas digitales (tanto desde el punto de vista empresarial como del consumidor) dio lugar a una serie de nuevas vulnerabilidades, que remodelaron radicalmente el panorama del fraude en el sector del retail. ¿Cómo? Los atacantes le siguen la pista al dinero, y durante la pandemia, ese dinero pasó a utilizarse de forma online más que nunca.

La demanda sin precedentes de determinados productos, como papel higiénico, desinfectantes, leche de fórmula para bebés y equipos para entrenar en casa, creó oportunidades lucrativas para que los operadores de bots aprovecharan estas condiciones. Por ejemplo, los bots scrapers acapararon artículos muy demandados para revenderlos a precios inflados, lucrándose con la escasez y la alta demanda de los consumidores.

Hasta este punto, los bots scrapers no estaban causando un daño generalizado significativo y eran bastante perceptibles. Esto permitió afrontarlos fácilmente con herramientas de seguridad tradicionales. Sin embargo, como eran el primer paso en un ataque de acaparamiento de inventario y este acaparamiento era tan rentable, los operadores de bots decidieron invertir una cantidad significativa de recursos para hacer que los scrapers fueran más evasivos.

Al mismo tiempo, los avances en el aprendizaje automático y la IA crearon una tormenta perfecta para que los atacantes lograran su objetivo. También aumentó la capacidad de lanzar varios ataques a la vez, utilizando sofisticadas técnicas de evasión, como la rotación de direcciones IP y proxies, para eludir los sistemas tradicionales de detección de bots. **Como señala Richard Meeus, director de Estrategia y Tecnología de Seguridad en EMEA de Akamai: *"Los bots son cada vez más inteligentes. Pueden imitar exactamente a un ser humano, y pueden entrar y salir antes incluso de que los hayas visto, lo que hace que sean más difíciles de detectar y combatir. También llegan en cantidades enormes, procedentes de miles de sitios distintos. Ningún retailer está a salvo".***

El aumento astronómico de las transacciones online causado por la pandemia (la cuota de ventas de retail online globales del total de ventas de retail creció de media de un 16 % al 19 % en 2020) también registró un aumento de formas de fraude más directas, como el robo de cuentas (ATO) y los ataques de phishing diseñados para robar información confidencial. Los retailers se enfrentaron al desafío de tener que distinguir entre interacciones legítimas con los clientes y actividades de bots maliciosos, y los atacantes maliciosos aprovecharon esas debilidades en la pila tecnológica del retail.

Desafortunadamente, estas susceptibilidades han llegado para quedarse. Los retailers tienen dificultades para seguir el ritmo de la evolución del fraude y el uso indebido digitales, que están creciendo más rápido que nunca. Y con el crecimiento del e-commerce global (que representa aproximadamente el 22 % de las ventas de retail globales en 2024, y que se prevé que crecerá hasta el 27 % en 2026), la responsabilidad de proteger la creciente cantidad de clientes legítimos que compran online recae sobre los retailers.

Sección 2: Cómo las actividades maliciosas reducen los ingresos del sector del retail y erosionan la confianza de los consumidores

Las actividades maliciosas en los retailers afecta fundamentalmente a los resultados netos. Según un estudio reciente, los comerciantes incurren en un **coste promedio de 3 $ por cada 1 $ de fraude**. Las cifras más recientes de 2023 indican que el coste total del fraude en el sector del e-commerce **supera en todo el mundo los 48 000 millones de dólares**, frente a los **41 000 millones de dólares de 2022**. Las pérdidas acumuladas por fraude en pagos online en todo el mundo aumentarán a más de **343 000 millones de dólares**. Para poner estos datos en perspectiva, eso es más del triple de los ingresos netos de Apple en 2023.

Y ese es solo el impacto financiero obvio: también hay un impacto en un valor que no se puede evaluar minuciosamente (y posiblemente mucho más costoso), y que implica perder ventaja competitiva, y erosionar el valor de la marca, la fidelidad y la confianza. Por lo tanto, ¿cómo y dónde se manifiesta en el negocio?

El papel del scraping en socavar las estrategias de precios y la exclusividad

El scraping, la práctica de extraer datos de sitios web mediante bots automatizados, supone una amenaza significativa para las marcas de los retailers, las estrategias de precios y la exclusividad de los productos. Y en el caso de muchas organizaciones de retail, ni siquiera saben que tienen un problema de scraping o, lo que es peor, no se dan cuenta del verdadero impacto que este tipo de actividad tiene en el negocio.

A continuación se muestran seis formas en las que el scraping puede perjudicar a su negocio:

1. Supervisión y reducción de precios

La competencia puede utilizar bots de scraping para supervisar continuamente la información de precios de un retailer. Con estos datos, pueden ofrecer unos precios más bajos, lo que dificulta para el retailer mantener una ventaja competitiva o implementar de manera eficaz estrategias de precios dinámicas.

2. Desventajas competitivas

Profundizando más en este punto, el scraping de datos de precios, productos e inventarios permite a la competencia obtener información valiosa sobre las estrategias de un retailer, lo que les permite ajustar sus propias tácticas en consecuencia y obtener una ventaja injusta. El terreno de juego ya no está nivelado.

3. Pérdida de exclusividad y valor de la marca

¿Sabe cuánta sangre, sudor y lágrimas ha invertido su equipo de marketing en la creación de imágenes y descripciones de productos? Los bots de scraping pueden extraer esta información y otro contenido confidencial del sitio web de un retailer. Este contenido robado se puede utilizar para crear listings falsificados o no autorizados en mercados de terceros o incluso sitios web similares, lo que socava la exclusividad y el valor de la marca.

En un nivel más amplio, se trata de un problema de suplantación de marca. Algunos de los distribuidores no son maliciosos, pero muchos de ellos sí lo son, y configuran estas páginas únicamente para robar información de tarjetas de crédito. Y su consumidor no sabe cuál es la diferencia.

4. Acaparamiento de inventario

Los bots pueden extraer datos de inventario en tiempo real y eludir los límites de compra o los sistemas de colas, lo que les proporciona una ventaja injusta sobre los clientes humanos. Como se ha mencionado anteriormente, esto permite a los revendedores o especuladores acaparar artículos de edición limitada o de gran publicidad, como PlayStations, productos de belleza o zapatillas, impidiendo a los clientes legítimos efectuar compras. Incluso si pueden, muchos de estos distribuidores subirán el precio 3 veces o hasta más, lo que provocará malestar entre los clientes fieles.

5. Niveles de inventario inexactos

Los bots que acaparan o compran grandes cantidades de productos pueden agotar rápidamente los niveles de inventario y provocar que se agoten las existencias (así como decepcionar a los clientes). Esto tiene un efecto negativo adicional en la previsión de ventas.

6. Métricas de marketing sesgadas

Estos bots actúan como humanos y sus análisis los reflejarán como tales, lo que sesga sus datos de marketing. Para uno de los clientes de Akamai, resultó que el 90 % de su tráfico eran bots, lo que tuvo un gran impacto en sus campañas de marketing y en los costes de la nube.

Christine Ross, directora de Marketing de Productos de Akamai, destacó: "En ocasiones, los clientes nos han dicho que un producto aparecía constantemente en las búsquedas en sus sitios web y que, por lo tanto, debía ser un producto realmente popular. Pero en realidad son bots los que lo están viendo y no humanos. Así que compraron más de un producto en particular porque el sitio web decía que era popular, pero de hecho, la gente no lo estaba comprando. No eran personas las que estaban viendo esa página. Esto afecta a las decisiones importantes de optimización de inventario y sitios web. Y a veces, si no extraes los datos de los bots, estás llevando a cabo la optimización para los bots y no para los consumidores. Esto puede eliminar el ROI en marketing y dificultar el crecimiento empresarial".

Disminución del rendimiento del sitio y sus repercusiones en la participación de los usuarios

Otra área muy afectada es el rendimiento del sitio web, la ventana del retailer al mundo. Los bots que realizan el scraping o acaparan el inventario pueden sobrecargar la infraestructura del sitio web de un retailer y ocasionar tiempos de carga más lentos, un aumento de los costes de los servidores e incluso interrupciones en el sitio. Esta degradación del rendimiento afecta directamente a la participación de los usuarios, ya que es probable que los clientes que se enfrentan a la carga lenta de páginas o al tiempo de inactividad abandonen el sitio, y podrían recurrir a la competencia.

Si tenemos en cuenta el hecho de que la media de páginas vistas por sesión de compra superó la cifra de 20 en 2023, lo que subraya la necesidad de más páginas y contenido para la conversión, cada vez es más crucial tener un sitio web de alto rendimiento. La frustración de los usuarios con los sitios web del sector del retail es real y está muy extendida, y afecta al 40 % de las experiencias de los compradores. Esto está directamente relacionado con la conversión, y cuesta a los retailers casi 0,60 dólares por visita en gasto desperdiciado.

Una mala experiencia de usuario también es enemiga de la retención. Los clientes recurrentes se convierten cuatro veces más que los clientes nuevos y tienen menos probabilidades de proceder de canales de pago. Si usted es un responsable de marketing que está haciendo malabarismos con un presupuesto ajustado, este es un punto clave en todo este asunto.

Cuentas vulneradas y los costes financieros y de reputación asociados

Los ataques de Credential Stuffing basados en bots y las campañas de phishing pueden dar lugar a la vulneración de las cuentas de los clientes, lo que resulta especialmente perjudicial. Estas credenciales robadas se pueden utilizar para el robo de cuentas, el robo de identidad o incluso la filtración de datos, todo lo cual afecta a las finanzas y la seguridad de los clientes, y la culpa recae directamente sobre usted.

Desde el punto de vista de los retailers, el acceso no autorizado a las cuentas puede dar lugar inmediatamente a pedidos fraudulentos y reembolsos, robo de puntos de fidelidad, uso indebido de cupones/promociones, reventa de cuentas y ataques de validación de CVV, entre otros. Entre las consecuencias a largo plazo del robo de cuentas se pueden incluir la sustitución de activos para los clientes, las posibles multas, la disminución de la confianza en la marca, el aumento de los costes de investigación del fraude y el agotamiento de los equipos encargados de la seguridad, el marketing y la lucha contra el fraude.

En lo que respecta a las filtraciones de datos, los costes financieros necesarios para solucionar el problema incluyen:

Aumento de los costes operativos

Por ejemplo, los costes relacionados con la seguridad, el cumplimiento o incluso, como en el caso de Neiman Marcus en 2021, la creación de un centro de llamadas dedicado para atender las quejas de los clientes sobre cómo se vieron afectados.

Servicios de reembolsos y supervisión del crédito

para los clientes afectados: un ejemplo de esto incluye el caso de Hudson Bay en 2018, que ofreció servicios de protección de la identidad a los clientes afectados.

Honorarios legales e indemnizaciones

Tras una filtración en 2013 de información de tarjetas de pago, el gigante del retail Target tuvo que hacer frente a una serie de demandas por un valor de casi 300 millones de dólares. El impacto en su crecimiento fue grave: las ganancias de Target cayeron casi un 50 % en el cuarto trimestre de ese año en comparación con el año anterior y el precio de sus acciones cayó un 9 % en el periodo de dos meses posterior.

Multas e investigaciones normativas

En el caso de Target, el Departamento de Justicia inició una investigación. Cuando en 2018, Dixons Carphone se vio involucrada en la filtración de la información de 14 millones de clientes, la Oficina del Comisario de Información del Reino Unido les impuso la sanción máxima de 500 000 libras.

Los costes para la reputación por las cuentas vulneradas y las filtraciones también afectan al crecimiento general. El 54 % de los clientes asegura que cambiarían a otra marca si la que utilizan sufre una filtración de datos. En el caso de las empresas que cotizan en bolsa, sufren una pérdida media del 3,5 % sobre el precio de sus acciones después de una filtración. En el caso de Dixons Carphone, la disminución de los beneficios llevó al cierre de 100 tiendas Carphone Warehouse en el plazo de un año y la totalidad de la marca Carphone Warehouse en 2020.

Las cuentas vulneradas son un factor importante en la percepción, la confianza y la fidelidad de los clientes, que constituyen el núcleo de los objetivos de cada responsable de marketing y marca. Por ejemplo, la percepción que tenían los consumidores de Target antes de la filtración de datos se situaba en un 20,7 en la clasificación Brand Index Buzz, y se desplomó a un mínimo de 9,4 el año siguiente. Cinco años más tarde, ascendió a 17,3, lo que permite hacerse una idea del esfuerzo necesario para recuperar su posición entre los consumidores. En el entorno actual, conectado y saturado de redes sociales, la percepción de la marca puede mejorar o desplomarse en cuestión de minutos.

El cambio en el comportamiento de los consumidores, junto con la crisis del coste de la vida, también ha afectado negativamente a la fidelidad de los consumidores. La confianza, una puerta de entrada a la fidelidad, es clave para ganarse a la próxima generación de consumidores y fomentar el crecimiento sostenible del negocio. Los millennials y la generación Z tienen los niveles más bajos de confianza en las marcas, lo que se puede atribuir quizás al hecho de que aproximadamente el 20 % de ellos han llegado a saber que han sufrido una filtración de sus datos (en comparación con el 2 % de la generación X y el 10 % de los baby boomers).

Por lo tanto, este fomento de la confianza requiere experiencias rápidas, fluidas y libres de fraude. Los compradores están dispuestos a pagar un 46 % más con un retailer en el que confían. ¿Cuál es el factor más importante para lograr esa confianza? Un proceso de pago seguro y la protección de los datos personales. Según un estudio global de 2023, casi el 90 % de los consumidores afirma que esto es vital para que los retailers logren ese objetivo. Una sólida reputación de la marca también ocupó un lugar entre los primeros puestos, con un 76 %.

Conclusión: Combatir los bots y el uso indebido con una organización alineada

Dado el aumento desenfrenado de estas tecnologías maliciosas, la tarea puede parecer otro desafío monstruoso que abordar. Pero no tiene por qué serlo. La buena noticia es que existen maneras efectivas para mantener el control sobre su propia marca y mejorar la experiencia del cliente. Pero ¿por dónde debe empezar?

Estrategias para proteger su marca y sus resultados netos

No es de extrañar que los distintos equipos se centren normalmente en proteger diferentes resultados: el de seguridad protege los datos, el de marketing protege los ingresos, el de TI protege contra las interrupciones y el de experiencia del cliente protege la experiencia de compra. Sin embargo, estos equipos tienen que enfrentarse a varios desafíos:

- *¿Se comunican y están en sintonía respecto de los resultados y objetivos empresariales compartidos?*
- *¿Pueden responder a la siguiente pregunta?: "¿Están las partes interesadas alineadas con respecto a los requisitos técnicos y las herramientas necesarias para proteger los datos de los clientes, la marca y los ingresos?"*

La mayoría de las veces nos encontramos con que la respuesta es que no, pero este factor es fundamental. Otras preguntas clave a las que estos equipos deben responder de forma colectiva son las siguientes:

- *¿Cuáles son los resultados que intentamos conseguir? (Por ejemplo, proteger los ingresos, los datos de los clientes, la experiencia de compra, contra el fraude, etc.).*
- *¿Necesitamos una o varias soluciones para resolver los distintos desafíos y casos de uso de las partes interesadas?*
- *¿Hay alguna desconexión entre el equipo que compra la solución y el que la utiliza realmente?*
- *¿En qué consiste tener éxito? ¿Tenemos KPI claramente definidos?*
- *¿Qué es lo que estamos dispuestos a tolerar/qué debemos sacrificar para encontrar un perfecto equilibrio entre la seguridad y la necesidad de optimizar la experiencia de compra?*
- *¿Estamos protegiendo toda nuestra infraestructura (sitio web, aplicación móvil, API e infraestructura)?*
- *¿Cómo gestionamos la frontera entre lo que deseamos y lo que no, y el límite difuso que hay entre ambos?*

Cada equipo necesita comprender estos puntos y tener un objetivo compartido que impulse la alineación y la acción con el fin de obtener resultados óptimos para la empresa.

El fraude en el sector del retail se está acelerando a un ritmo sin precedentes y tiene un impacto generalizado en los retailers. Como hemos indicado, las pérdidas van más allá de las que se ven fácilmente en un libro de contabilidad como consecuencia de multas, indemnizaciones u honorarios legales. Se trata del objetivo principal del retailer de aumentar los ingresos a través de la marca y la fidelidad de los clientes. La marca y la fidelidad dependen de la confianza y la experiencia del cliente, factores que disminuyen en un abrir y cerrar de ojos por las actividades fraudulentas.

El aumento del uso indebido, junto con un difícil panorama de compras de los consumidores y el constante aumento de las ventas online, significa que es más importante que nunca que los retailers prioricen e inviertan en medidas de seguridad avanzadas para proteger su marca y a sus clientes. Esto significa que las unidades de negocio deben colaborar para comprender y compartir el impacto que tienen los ataques maliciosos, porque la responsabilidad ya no recae exclusivamente en los equipos de seguridad y TI.

Si necesita ayuda, póngase en contacto con el equipo de Akamai u obtenga más información sobre las soluciones para los sectores del retail, el turismo y la hostelería. Akamai ha ayudado a retailers y marcas globales como Lufthansa, Wagner eCommerce Group, Panasonic y TOUS a ofrecer experiencias online seguras y atractivas durante más de 25 años.

Acerca de Akamai

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. Akamai Connected Cloud, una plataforma de Edge y en la nube de distribución masiva, acerca las aplicaciones y las experiencias a los usuarios y aleja las amenazas. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn.

Este documento se ha redactado en colaboración con Retail Gazette, la mayor publicación del sector del retail de empresa a empresa (B2B) del Reino Unido.

Visite **www.retailgazette.co.uk** para unirse a otros 300 000 usuarios mensuales de forma gratuita y acceder a los últimos informes detallados, noticias, entrevistas, análisis, y documentos técnicos.

Publicado en julio de 2024