CLOUDFLARE

DOCUMENTO TÉCNICO

Manual de estrategias de bots maliciosos: señales de alerta temprana y cómo actuar

Contenido

Introducción

En la actualidad, los bots representan alrededor del 30 % del tráfico en línea, y el objetivo de muchos de esos bots es dañar a organizaciones como la tuya, con un estimado del 93 % de ese tráfico de bots sin verificar y potencialmente malicioso. La prevalencia del robo del contenido y los precios, la usurpación de cuentas, el relleno de credenciales y tarjetas de crédito, la acumulación de inventario y los ataques DDoS impulsados por la red de robots (botnet) indica que los actores de bot maliciosos son cada vez más complejos y sofisticados cada año.

Además, las medidas tradicionales contra los bots, como el bloqueo de ubicación, el bloqueo de direcciones IP y los CAPTCHA tradicionales, son ineficaces hoy en día. De hecho, los CAPTCHA son más fáciles de resolver para los bots que para los humanos.[1]

Por esta razón, ninguna táctica específica puede detener a todos los bots y evitar que dañen a tus usuarios y a tu marca. El único método eficaz es estar alerta a una variedad de señales de advertencia reveladoras de bots, y responder a cada una de ellas con una recopilación de datos y con la implementación de respuestas específicas, detección de patrones, análisis predictivos y otras estrategias complementarias.

1. https://www.usenix.org/conference/usenixsecurity23/presentation/searles

Señales de alerta de un problema de bots

Si haces un seguimiento de una serie de indicadores potenciales, tendrás una excelente oportunidad de detectar bots maliciosos antes de que generen un daño grave. Debes buscar:

Mayores costos de infraestructura sin aumento de la actividad comercial

Todo el tráfico que se dirige a tu sitio web tiene un costo. Con la independencia de quién o qué acceda a tu contenido, tienes que asumir los costos de almacenamiento y procesamiento. Pero los bots maliciosos pueden aumentar los costos relacionados con tu tráfico sin aportar ingresos a tu negocio. Si bien los bots buenos son utilizados por los motores de búsqueda para indexar contenido en tu sitio web y brindar soporte a tu clasificación de SEO, los bots maliciosos aumentan excesivamente los cargos de ancho de banda cada año.

Compras inusuales de inventario de bajo volumen y alta demanda

Si adviertes que estás vendiendo, de modo sospechoso, un porcentaje alto de tu inventario a un subgrupo sorprendentemente pequeño de compradores, es posible que los bots que acumulan inventario sean los responsables. Si bien algunos de estos bots solo llenarán y abandonarán los carritos de compra para bloquear a los clientes legítimos, otros comprarán tu inventario con el objetivo de revenderlo a un precio más alto en otros sitios.

Aumento de las quejas de los clientes

Un aumento de las solicitudes de soporte relacionadas con los bloqueos de cuentas y las transacciones fraudulentas podría ser un indicio de bots de relleno de credenciales. Estos bots se apoderan de las cuentas de usuario legítimas con la información que han recopilado de fugas anteriores. Además de generar un impacto negativo en la experiencia de tus clientes, estas transacciones fraudulentas sobrecargarán tus servidores, con tiempos de carga de la página más largos, o incluso harán que tu sitio web quede fuera de servicio.

Aumento de los intentos de inicio de sesión fallidos

Todos los clientes introducen contraseñas erróneas de vez en cuando, pero si adviertes una serie repentina de intentos fallidos de inicio de sesión, es muy probable que tengas un problema de bots. Si bien algunos bots de relleno de credenciales intentan acceder a las cuentas de clientes legítimos con credenciales robadas, una técnica más sencilla y frecuente es lanzar ataques con contraseñas por fuerza bruta, en el que los bots intentan muchos inicios de sesión rápidos mediante diccionarios de miles de nombres de usuario y contraseñas populares. Cuando un bot excede el límite de inicios de sesión fallidos de tu sitio para una cuenta en particular, el verdadero propietario de esa cuenta quedará bloqueado hasta que resuelvas el problema, lo cual afectará la experiencia de usuario.

Bajo rendimiento de la inversión en publicidad

La publicidad digital puede ser una herramienta eficaz para dirigir tráfico a tu sitio, pero también es un arma lucrativa para los bots maliciosos. Muchos bots de tráfico imitan el comportamiento de usuarios reales: hacen clic repetidamente en tus anuncios para aumentar tu inversión de pago por clic (PPC) y luego abandonan el sitio sin realizar una compra. Si bien algunas plataformas publicitarias han implementado algoritmos de aprendizaje automático para reducir el fraude de clics, gran parte de este sigue sin ser detectado.[2] Por eso es crucial ser proactivo y supervisar cada clic que llega a través de tus anuncios.

Análisis de visitas de página sesgadas

Si las visitas a tus páginas aumentan repentinamente sin motivo aparente, los bots maliciosos podrían ser los responsables. Si bien un aumento en el tráfico puede provenir de usuarios humanos cuando acabas de lanzar un nuevo producto o un evento de promoción, los operadores de bots maliciosos son cada vez más inteligentes en cuanto a la implementación de bots de apropiación de contenido justo en esos momentos, roban tu contenido y afectan de manera negativa tu análisis de datos globales.

Aumento repentino de creación de cuentas

Cuando cientos o miles de cuentas de usuario nuevas aparecen de repente, es posible que se trate de bots. Pueden usar estos perfiles falsos para enviar spam a tus calificaciones públicas y cometer muchas otras formas de fraude, lo que pone en riesgo no solo tus ingresos y retención de usuarios, sino también la credibilidad de tu marca.

Duplicados de tu contenido en sitios no aprobados

Que otros sitios compartan tu contenido puede ser bueno, pero un aumento repentino del contenido duplicado es un indicio de bots de apropiación de contenido. Estos bots roban información que te ha llevado tiempo reunir y organizar, y permite a los operadores de sitios maliciosos alojarla en dominios de su propiedad y aumentar su propio tráfico, mientras el tuyo se ve afectado.

Tráfico procedente de ubicaciones geográficas inusuales

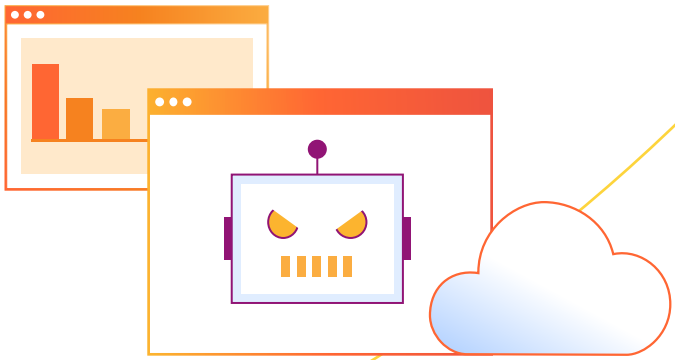
Los picos repentinos procedentes de ubicaciones inesperadas pueden ser un indicio de bots maliciosos, en especial, si esta actividad aparece en clústeres, centrada en regiones en las que no viven tus clientes o en las que tus servicios no están disponibles. Debes estar atento a cualquier actividad sospechosa que no esté relacionada con tu base de usuarios habituales.

Tráfico desde ubicaciones habituales en horarios inusuales

Así como los picos de tráfico desde lugares inesperados pueden ser indicios de bots maliciosos, los picos de tráfico desde lugares habituales en horarios inusuales pueden indicar que los bots están tratando de hacerse pasar por usuarios habituales. Si observas un aumento en la actividad desde una región habitual en la mitad de la noche, por ejemplo, debes investigar más en detalle ese tráfico.

Aumento en los errores de validación de tarjetas

Una señal particularmente peligrosa de bots maliciosos es un aumento en las transacciones con tarjetas de crédito que no se pueden validar. Los bots de relleno de tarjetas de crédito probarán miles de números de tarjetas de crédito robadas en un intento por encontrar una que funcione. Para hacerlo, efectúan compras de bajo valor en sitios web menos seguros, antes de hacer transacciones más grandes en sitios más importantes, o venden los números de tarjetas validadas en la Dark Web. Tu sitio puede incluirse en estos planes en cualquier momento de la cadena, y si las transacciones fallidas son muy notorias, tu proveedor de pagos puede multarte.



2. 1 https://www.entrepreneur.com/article/313943

Tácticas para combatir los bots

Como no hay dos ataques de bots iguales, en general, necesitarás una combinación de tácticas para detener su avance. Considera algunas de las siguientes estrategias:

Bloquear los bots maliciosos apenas los detectas

La respuesta más clara a un bot es también una de las más efectivas: solo bloquea todo el tráfico que hayas identificado como proveniente de actividades de bots maliciosos. Por sí sola, esta táctica puede ahorrarte costos significativos en ancho de banda y almacenamiento, además de proteger al consumidor y la reputación de tu marca. Además, recuerda que si un operador de bots está muy motivado, puede cambiar de táctica e intentarlo más tarde con una estrategia de ataque diferente.

Incluir en una lista de permitidos todos los bots buenos que conoces

Incluso cuando detectas y bloqueas los bots maliciosos, es fundamental que te asegures de que los bots buenos de los motores de búsqueda y los socios puedan rastrear tu sitio web. Esto no solo garantiza que tu posicionamiento de SEO siga siendo sólida, sino que también mantiene un buen flujo de tráfico de clientes legítimos de servicios de terceros que te envían tráfico a tu sitio web. Las listas de los permitidos también facilitan el establecimiento de normas de bloqueo de bots que no afectan, de manera negativa, el acceso de visitantes reales.

Desafiar a los bots sospechosos que detectas

Apenas observes un patrón de inicios de sesión sospechosos, baja profundidad de la página o del tiempo en la página, validaciones fallidas de tarjetas de crédito, o cualquier otro comportamiento típico de los bots maliciosos, debes implementar una prueba de seguridad. En el pasado, el envío de desafíos CAPTCHA se consideraba una práctica recomendada. Sin embargo, muchos bots avanzados ahora pueden resolver estas pruebas incluso más rápido y con mayor precisión que los usuarios humanos.

Hoy en día, el mejor enfoque es utilizar desafíos sin CAPTCHA, en los que el software de "desafío" tiene en cuenta una serie de factores para determinar si el usuario es realmente un bot (p. ej. red, dispositivo, huellas digitales de JavaScript).
Idealmente, los desafíos “No CAPTCHA” como este se integran con una solución completa de gestión de bots para obtener la máxima precisión (ver la sección Conclusión para obtener más información)

Limitar la velocidad a la que los usuarios pueden solicitar información

La limitación de velocidad puede ser una técnica efectiva para mantener bajo control a los bots menos sofisticados. Al establecer límites estrictos en cuanto a la cantidad de veces que una dirección IP puede enviar solicitudes a tu sitio, evitarás muchos ataques simples de fuerza bruta de bots, que intentan iniciar sesión usando miles de palabras del diccionario y contraseñas comunes. Sin embargo, los bots más avanzados pueden mantener su cantidad de solicitudes por debajo de tu limitación de velocidad, y no se los puede detectar mientras continúan provocando daños.

Llevar registros detallados de todo el tráfico del sitio

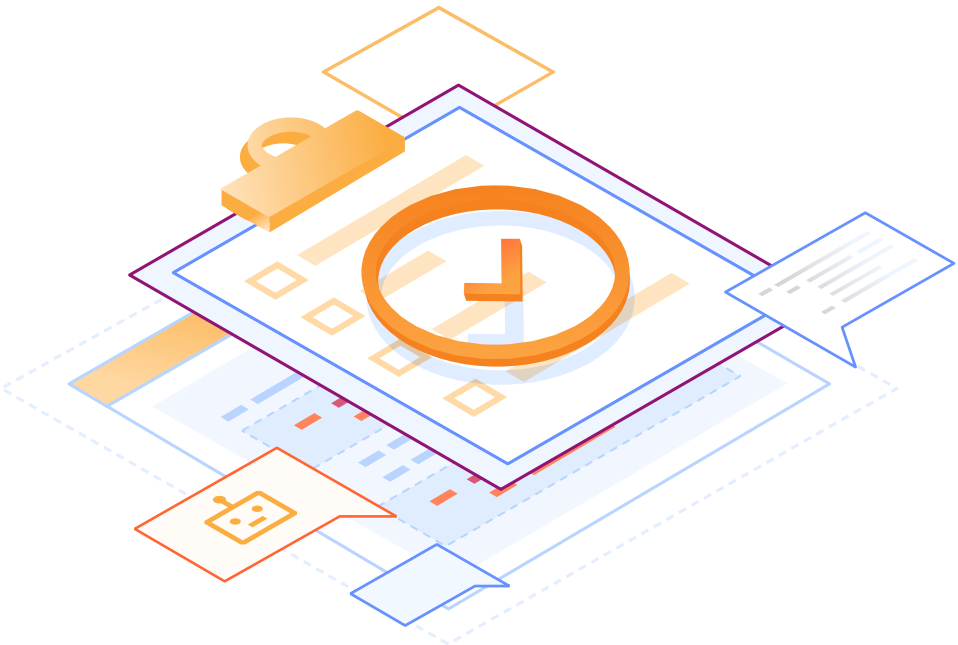
Si bien es probable que lleves registros diarios de visitas a las páginas e inicios de sesión en las cuentas, un tipo de registros más detallados de la información de los usuarios, tales como direcciones IP, navegadores, dispositivos, sistemas operativos, geolocalizaciones, referentes, redes y visitas de páginas, pueden resultar invaluables para detectar patrones de actividad más sutiles. Los registros pueden darte una idea clara de cómo suelen comportarse los bots en tu sitio y te permiten establecer políticas de seguridad más efectivas. Además, los registros suelen ser esenciales para informar y cumplir con las normativas en caso de que sufras una fuga de datos.

Redireccionar los bots al contenido alternativo

Cuando estás bastante seguro de que una determinada fuente de tráfico es un bot, ofrece contenido alternativo que consuma sus recursos informáticos. Incluso puedes ofrecer datos falsos, como información de precios errónea, a los bots que se apropian del contenido, para hacer que resulten inútiles para sus operadores. Técnicas como estas te darán tiempo para observar el comportamiento de los bots, para entender el patrón de actividad y para preparar una estrategia para acabar con ellos de una vez.

Exigir una autenticación adicional para todos los usuarios

A medida que los ataques de bots se hacen más frecuentes, cada vez más sitios recurren a medidas de seguridad más estrictas, incluso para los accesos de usuarios humanos legítimos. La autenticación de dos factores (2FA), por ejemplo, exige que los usuarios confirmen su identidad en varios dispositivos o cuentas, mientras que las contraseñas de un solo uso (OTP) pueden desalentar a los bots de relleno de credenciales porque hacen que el acceso a las cuentas sea más difícil de descifrar. Pero recuerda que estas técnicas pueden tener un impacto negativo en la experiencia del usuario y generar inconvenientes en el proceso de inicio de sesión.

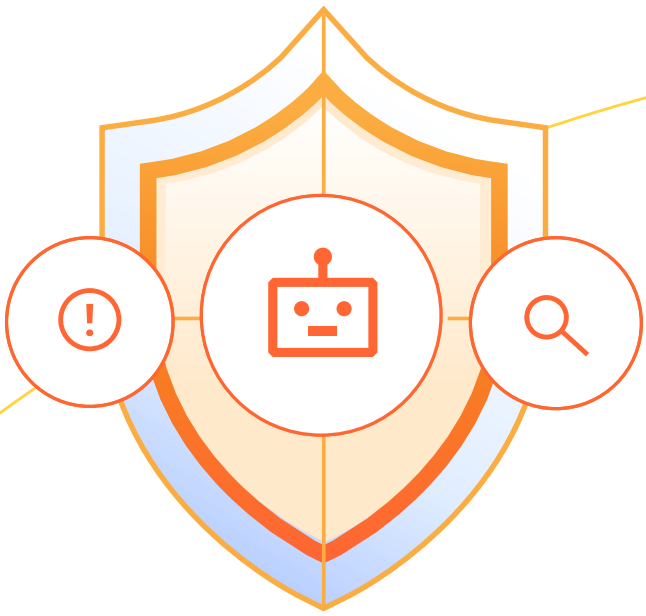


Conclusión

Cuando explores estas tácticas, recuerda que ninguna de ellas detendrá a los bots como un único enfoque. Para proteger tu empresa, es probable que debas combinar tácticas y agregar un análisis avanzado de patrones de múltiple variables. La gestión de bots de Cloudflare puede ayudar a organizaciones de diversos sectores a adoptar este enfoque multifacético. Está integrada a la amplia red de Cloudflare, y admite millones de propiedades de Internet y se extiende a más de 330 ciudades en todo el mundo.

Al aprovechar la información sobre amenazas continua de toda esa red, la gestión de bots de Cloudflare ofrece un análisis de comportamiento, aprendizaje automático y huellas digitales del lado del cliente para reducir significativamente el esfuerzo de combatir los bots maliciosos. Además, Cloudflare ofrece Turnstile, un desafío de bots sencillo y sin CAPTCHA, que se puede integrar en cualquier aplicación web con solo unas pocas líneas de código.

Más información acerca de la gestión de bots de Cloudflare.



+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/es-LA

REV:BDES-6333.2024SEPT03