CLOUDFLARE

СПРАВОЧНЫЙ ДОКУМЕНТ

Практическое руководство по вредоносным ботам: ранние признаки и способы противодействия

Содержание

3 Введение

4 Признаки наличия проблемы с ботами

6 Тактика борьбы с ботами

8 Заключение

Введение

Сегодня на долю ботов приходится около 30 % онлайн-трафика, и многие из этих ботов стремятся нанести ущерб таким организациям, как ваша, причем, по оценкам, 93 % этого трафика ботов не проверено и потенциально вредоносно. Распространенность скрапинга контента и цен, захвата учетных записей, атаки с использованием украденных учетных данных и данных кредитных карт, скупки или резервирования товаров, а также распределенных DDoS-атак на основе ботнета указывает на то, что злоумышленники, использующие боты, с каждым годом становятся все более изощренными.

Кроме того, традиционные меры по борьбе с ботами, такие как блокировка по местоположению, блокировка IP-адресов и традиционные CAPTCHA, сегодня неэффективны. На самом деле, ботам проще пройти CAPTCHA, чем людям.[1]

По этой причине нет единой тактики, которая могла бы остановить всех ботов и предотвратить нанесение ущерба вашим пользователям и вашему бренду. Единственный эффективный подход — это быть начеку и обращать внимание на различные признаки, указывающие на наличие ботов, и реагировать на каждый из них, собирая данные, а затем применяя целевые меры, обнаружение закономерностей, прогнозную аналитику и другие дополнительные стратегии.

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

Признаки наличия проблемы с ботами

Отслеживая ряд потенциальных индикаторов, вы получаете отличную возможность обнаружить вредоносных ботов, прежде чем они нанесут серьезный ущерб. Вот на что следует обратить внимание:

Рост затрат на инфраструктуру без роста бизнеса

Любой трафик на ваш сайт связан с определенными затратами. Независимо от того, кто или что получает доступ к вашему контенту, вам придется оплачивать расходы на хранение данных и вычисления. Но вредоносные боты могут увеличить ваши расходы, связанные с трафиком, не принося никакого дохода вашему бизнесу. В то время как полезные боты используются поисковыми системами для индексации контента на вашем сайте и, таким образом, поддерживают ваш SEO-рейтинг, вредоносные боты каждый год значительно увеличивают расходы на пропускную способность.

Необычные покупки ограниченных товаров высокого спроса

Если вы заметили, что продаете подозрительно высокий процент своего ассортимента необычно небольшому количеству покупателей, виновниками этого могут быть боты, осуществляющие скупку или резервирование товаров. В то время как некоторые из этих ботов будут просто заполнять и затем бросать тележки для покупок, чтобы блокировать легитимных клиентов, другие фактически будут покупать ваш ассортимент с целью его перпродажи по более высокой цене на других сайтах.

Участившиеся жалобы клиентов

Увеличение количества обращений в службу поддержки, связанных с блокировкой учетных записей и мошенническими транзакциями, может быть признаком использования ботов, осуществляющих подстановку учетных данных. Такие боты перехватывают легитимные учетные записи пользователей с помощью информации, которую они собрали в результате прошлых утечек. В дополнение к негативному влиянию на удобство ваших клиентов, эти мошеннические транзакции приведут к перегрузке ваших серверов, и, соответственно, увеличению времени загрузки страниц, или даже сделают ваш веб-сайт недоступным.

Рост числа неудачных попыток входа в систему

Каждый пользователь время от времени ошибается при вводе пароля, но если вы наблюдаете внезапную череду неудачных попыток входа в систему, скорее всего, у вас проблема с ботом. В то время как некоторые боты, выполняющие подстановку учетных данных, пытаются получить доступ к легитимным учетным записям клиентов с помощью украденных данных для входа в систему, более простым и распространенным методом является атака методом перебора паролей (brute-force), в ходе которой боты пытаются выполнить множество быстрых входов в систему, используя словари тысяч популярных имен пользователей и паролей. Когда бот превысит установленный на вашем сайте лимит неудачных входов для конкретной учетной записи, реальный владелец этой учетной записи будет заблокирован до тех пор, пока вы не решите эту проблему, что является серьезным неудобством в отношении удобства пользователей.

Низкая эффективность рекламных расходов

Цифровая реклама может являться эффективным инструментом для привлечения трафика на ваш сайт, но это также и выгодное оружие для вредоносных ботов. Многие трафик-боты имитируют поведение пользователей: многократно нажимают на ваши объявления, чтобы увеличить ваши расходы с оплатой за клик (PPC), а затем уходят без совершения покупки. Несмотря на то, что некоторые рекламные платформы используют алгоритмы машинного обучения для сокращения кликфродов, большая часть таких кликов остается незамеченной.[2]
Вот почему так важно действовать на опережение и отслеживать каждый клик по вашим рекламным объявлениям.

Искажение аналитики просмотров страниц

Если количество просмотров вашей страницы внезапно резко возросло без видимой причины, то виновником этого могут быть вредоносные боты. Пик трафика может исходить от пользователей, в том случае, если вы только что запустили новый продукт или рекламную акцию, но операторы вредоносных ботов все более изощренными в развертывании ботов, осуществляющих скрапинг контента, именно в это время, крадут ваш контент и негативно влияют на ваши агрегированные аналитические данные.

Внезапное увеличение числа созданных учетных записей

Когда сотни или даже тысячи новых учетных записей пользователей появляются без видимой причины, за этим потоком могут стоять боты. Они могут использовать эти поддельные профили для рассылки спама в отношении ваших публичных рейтингов и совершения множества других форм мошенничества, угрожающих не только вашим доходам и удержанию пользователей, но и репутации вашего бренда.

Дублирование вашего контента на сторонних неавторизованных сайтах

Другие сайты, которые делятся вашим контентом, могут быть легитимными, но внезапное увеличение явного дублирования контента является отличительной чертой ботов, осуществляющих скрапинг контента. Эти боты крадут информацию, на сбор и обработку которой вы потратили время, позволяя операторам вредоносных сайтов размещать ее на принадлежащих им доменах, увеличивая их собственный трафик, в то время как ваш трафик страдает.

Трафик, исходящий из необычных географических местоположений

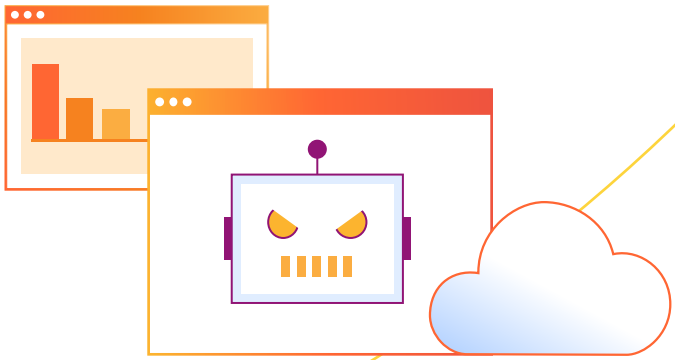
Внезапные пики трафика, возникающие из неожиданных местоположений, могут указывать на вредоносную активность ботов, особенно если эта активность проявляется в кластерах, сосредоточенных в регионах, где ваши клиенты не проживают или где ваши услуги недоступны. Внимательно следите за любой подозрительной активностью, которая кажется не связанной с вашей обычной пользовательской базой.

Трафик из типичных местоположений в необычное время

Точно так же, как пики трафика из неожиданных местоположений могут указывать на вредоносных ботов, пики из типичных мест в необычное время могут указывать на то, что боты пытаются замаскироваться под ваших обычных пользователей. Например, если вы наблюдаете всплеск активности из обычного региона посреди ночи, вы можете более внимательно изучить этот трафик.

Увеличение количества сбоев при проверках карт

Особенно опасным признаком вредоносных ботов является увеличение количества транзакций по кредитным картам, которые не проходят проверку. Боты, выполняющие подбор данных кредитных карт, перебирают тысячи украденных номеров, пытаясь найти работающий. Они делают это, совершая мелкие покупки на менее защищенных сайтах перед тем, как перейти к более крупным транзакциям на более крупных сайтах или за счет продажи проверенных номеров карт в даркнете. Ваш сайт может попасть в эту схему на любом этапе — и если число неудачных транзакций будет слишком велико, ваш платежный провайдер может оштрафовать вас.



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

Тактика борьбы с ботами

Поскольку не существует двух одинаковых атак ботов, вам, как правило, потребуется комбинация нескольких тактик, чтобы остановить их на ранней стадии. Рассмотрите некоторые из следующих стратегий:

Блокируйте вредоносных ботов сразу после их обнаружения

Наиболее очевидный ответ на действия бота также является одним из наиболее эффективных: просто заблокируйте весь трафик, который вы идентифицировали как исходящий от активности вредоносного бота. Уже одна эта тактика может сэкономить вам значительные средства на пропускной способности и хранении данных, не говоря уже о том, что она позволяет сохранить доверие клиентов и репутацию вашего бренда. В то же время помните, что если оператор бота обладает высокой мотивацией, он может изменить свою тактику и вернуться позже с другой стратегией атаки.

Добавьте все известные вам легитимные боты в белый список (allowlist)

Даже когда вы обнаруживаете и блокируете вредоносных ботов, крайне важно убедиться, что полезные боты из поисковых систем и партнерских сервисов по-прежнему имеют доступ к вашему сайту. Это не только гарантирует, что ваш SEO-рейтинг останется стабильным, но и обеспечит беспрепятственный поток легитимного клиентского трафика от сторонних сервисов, которые направляют к вам трафик. Список разрешенных адресов также значительно упрощает настройку правил блокировки ботов, которые не будут негативно влиять на доступ реальных посетителей.

Проверяйте обнаруженных подозрительных ботов

Как только вы заметите ряд подозрительных входов в систему, низкую глубину страницы или время пребывания на странице, неудачные проверки кредитных карт или любое другое поведение, характерное для ботов, необходимо провести тест безопасности. Ранее применение CAPTCHA считалось лучшей практикой. Однако многие усовершенствованные боты теперь могут решать эти «головоломки» даже быстрее и точнее, чем обычные пользователи.

Сегодня лучшим подходом является использование проверок без CAPTCHA, в которых программное обеспечение «проверки» учитывает множество факторов, чтобы определить, действительно ли пользователь является ботом (например, сеть, устройство, отпечатки JavaScript).
В идеале, подобные задачи «без CAPTCHA» интегрируются в комплексное решение по управлению ботами для обеспечения максимальной точности (подробнее см. в Заключении).

Ограничение скорости, с которой пользователи могут запрашивать информацию

Ограничение скорости может быть эффективным методом сдерживания менее изощренных ботов. Установив жесткие ограничения на количество запросов, которые любой IP-адрес может отправлять на ваш сайт, вы предотвратите множество упрощенных атак ботов, действующих методом подбора пароля, которые пытаются войти в систему, используя тысячи словарных слов и общие пароли. Однако современные более усовершенствованные боты могут поддерживать количество запросов чуть ниже установленного вами лимита скорости, оставаясь незамеченными, пока они продолжают наносить ущерб.

Ведение подробных журналов всего трафика сайта

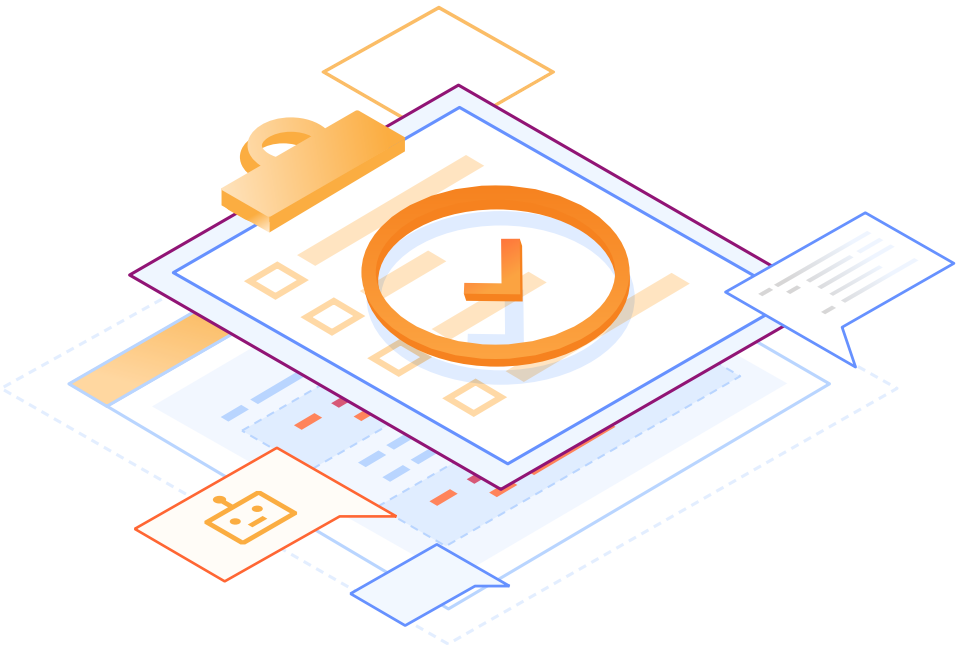
Несмотря на то, что вы, скорее всего, уже ведете ежедневные журналы просмотров страниц и входов в учетную запись, более подробные журналы информации о пользователях — такие как IP-адреса, браузеры, устройства, операционные системы, геолокации, ссылки, сети и просмотры страниц — могут оказаться бесценными для выявления более тонких моделей активности. Журналы могут дать вам четкое представление о поведении ботов на вашем сайте, что позволит вам разработать более эффективные политики безопасности. Кроме того, журналы часто необходимы для отчетности и соблюдения нормативных требований в случае, если вы действительно пострадаете от утечки данных.

Перенаправление ботов на альтернативный контент

Когда вы абсолютно уверены, что определенный источник трафика является ботом, предоставьте ему альтернативный фрагмент контента, который потребляет его вычислительные ресурсы. Вы даже можете подавать поддельные данные — например, ошибочную информацию о ценах — ботам, занимающимся скрапингом контента, делая их бесполезными для своих операторов. Подобные методы позволят вам выиграть время, чтобы понаблюдать за поведением каждого бота, понять характер его активности и подготовить стратегию, чтобы справиться с ним раз и навсегда.

Требование дополнительной аутентификации для всех пользователей

По мере того как атаки ботов становятся все более распространенными, все больше сайтов обращаются к повышенным мерам безопасности даже для легитимных входов в систему пользователей. Например, двухфакторная аутентификация (2FA), требует, чтобы пользователи подтверждали свою личность на нескольких устройствах или учетных записях, в то время как одноразовые пароли (OTP) могут препятствовать ботам, осуществляющим подстановку учетных данных, усложняя взлом учетных записей. Но помните, что такие методы могут негативно повлиять на удобство ваших пользователей, усложняя для них процесс входа в систему.

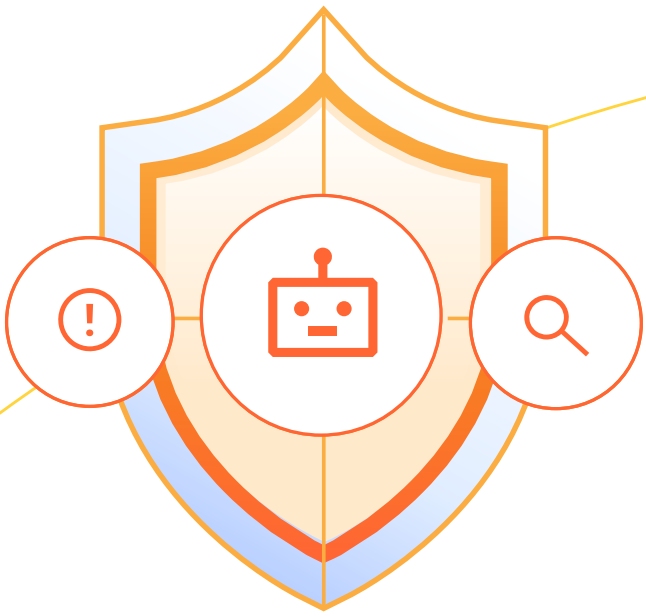


Заключение

Изучая эти тактики, помните: ни один из них не остановит всех ботов как самостоятельный метод. Чтобы защитить свой бизнес, вам, скорее всего, потребуется комбинировать тактики, а также добавить расширенный анализ многомерных моделей. Cloudflare Bot Management может помочь организациям из самых разных отраслей промышленности внедрить этот комплексный подход. Это решение интегрировано в более широкую сеть Cloudflare, которая поддерживает миллионы интернет-ресурсов и охватывает более 330 городов по всему миру.

Опираясь на непрерывную информацию об угрозах из этой сети, управление ботами от Cloudflare предлагает анализ поведения, машинное обучение и идентификацию клиентов по цифровым отпечаткам, что значительно упрощает борьбу с вредоносными ботами. Кроме того, Cloudflare предлагает Turnstile — почти незаметную проверку на бот без CAPTCHA, которую можно интегрировать в любое веб-приложение с помощью всего нескольких строк кода.

Узнайте больше об управлении ботами от Cloudflare.



+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/ru-ru/

REV:BDES-6333.2024SEPT03