CLOUDFLARE

ОБЗОР ПРЕДЛАГАЕМЫХ РЕШЕНИЙ

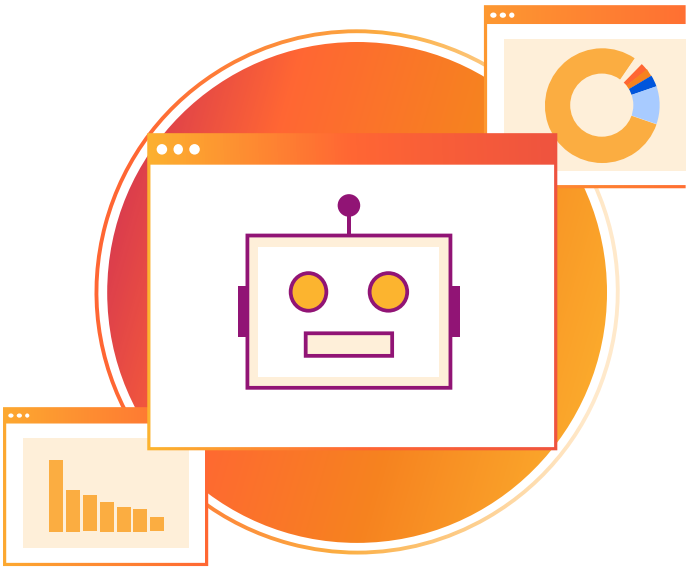
4 стратегии по управлению вредоносными ботами

Избегайте дорогостоящего ущерба и упущенного дохода вследствие действий нежелательных ботов

Боты присутствуют повсюду в Интернете

Боты распространены в современном Интернете, потому что они способствуют автоматизации важных задач. Согласно оценкам, 40–50 % всего интернет-трафика управляется ботами, и многие из этих ботов выполняют легитимные бизнес-функции.

Тем не менее, боты также часто используются преступниками для атаки на веб-ресурсы и причинения дорогостоящего ущерба. Вредоносные боты могут красть данные, взламывать учетные записи пользователей, отправлять нежелательные данные через онлайн-формы и выполнять другие вредоносные действия. Такие вредоносные боты расходуют драгоценные вычислительные ресурсы и ресурсы сайта, крадут данные и искажают аналитику трафика.



Что такое управление ботами?

Управление ботами означает блокировку нежелательного или вредоносного трафика ботов, при этом позволяя полезным ботам получать доступ к веб-ресурсам. Это достигается путем обнаружения активности ботов, различения желаемого и нежелательного поведения ботов, а также определения источников нежелательной активности.

Почему это важно?

Управление ботами необходимо, поскольку боты, если их не контролировать, могут вызвать масштабные и дорогостоящие проблемы. Организации должны убедиться, что они не блокируют нужных ботов, таких как роботы, сканирующие поисковые системы, в рамках своих усилий по фильтрации любого трафика вредоносных ботов на свои веб-ресурсы.

Что можно предпринять?

Выявление и блокировка вредоносных ботов до того, как они инициируют атаки, является важнейшим компонентом любой надлежащей стратегии безопасности. Мы поделились четырьмя историями реальных клиентов Cloudflare, которые решили свои проблемы с управлением ботами с помощью четырех разных стратегий, используя продукты Cloudflare.

Блокировка ботов

Такой подход требует осторожности, поскольку многие легитимные бизнес-процессы, например, индексация поисковых систем, требуют, чтобы боты имели доступ к ресурсам компании.

Блокировка ботов		
Проблема	**Решение**	**Результаты**
Компания, работающая в сфере онлайн-гейминга, заметила значительное увеличение количества жалоб от пользователей. Их учетные записи были взломаны, а информация о кредитных картах украдена. Злоумышленники использовали автоматизированных ботов для подбора учетных данных для входа в систему, получения доступа к учетным записям пользователей и, в конечном итоге, их захвата.	Команда безопасности применила **ограничение числа запросов** вместе с расширенным **управлением ботами** для обнаружения многочисленных попыток входа в систему за короткий промежуток времени. При обнаружении необычного поведения, ограничение числа запросов автоматически блокировало вредоносные запросы. С момента внедрения функции ограничения числа запросов компания, занимающаяся онлайн-играми, не подвергалась ни одной атаке типа «Подстановка учетных данных».	Все компании должны обеспечивать баланс между строгой безопасностью с оптимальным удобством для пользователя. Соответствующий набор инструментов может способствовать обнаружению и предотвращению вредоносного трафика ботов, сводя к минимуму ложные срабатывания и препятствия для реальных пользователей.

Замедление врага

Данная техника позволяет максимально увеличить время отклика на все подозрительные сетевые запросы.

Замедление врага		
Проблема	**Решение**	**Результаты**
Букмекерская компания заметила значительное сокращение количества транзакций. При анализе проблемы сотрудники компании выявили действия вредоносных ботов, которые выполняли скрапинг ставок на веб-сайте компании и использовали эту информацию для получения конкурентного преимущества.	Компания не блокировала ботов, потому что злоумышленники могли обойти блокировку. Вместо этого они замедлили получение данных для ставок. Они использовали **переопределение заголовков (Headers Override)** для маркировки подозрительных запросов на основе анализа **управления ботами**, а затем сценарии **Workers** для реагирования на эти заголовки и замедления запросов.	Этот метод позволил компании восстановить нормальную активность пользователей. Другие методы включают использование капчи для большого объема запросов или изменение HTML-разметки через регулярные интервалы. Эти действия прерывают рабочий процесс ботов, поэтому последовательный скрапинг контента становится более сложным.

Обман ботов

Несмотря на то, что многие компании используют средства противодействия ботам, по-настоящему изощренный злоумышленник может их обойти. Вместо этого некоторые компании решают дать отпор.

Обман ботов		
Проблема	**Решение**	**Результаты**
Букмекерская компания попыталась найти решение для ботов, выполняющих скрапинг ставок на своем веб-сайте. После некоторых раздумий ее сотрудники решили запустить обходное решение на основе нескольких продуктов Cloudflare, которое позволило бы им «скармливать» ботам рандомизированную информацию.	Когда система определила, что запрос был сгенерирован вредоносным ботом, она приняла этот запрос и сгенерировала новый рабочий процесс: Запрос → **WAF** (бот идентифицирован) → **Bot Management (Управление ботами)** (присвоен балл угроза) → **Workers** (генерировать рандомизированные данные) → **Workers** (вернуть рандомизированные данные боту)	Новый рабочий процесс генерировал новые рандомизированные данные, которые возвращались вредоносным ботам. В результате боты, которые приходили для того, чтобы собирать ставки и наносить ущерб, возвращались с бесполезными данными, что лишало смысла любые дальнейшие вредоносные действия.

Выполнение динамического анализа

Поскольку боты становятся все более изощренными, компаниям необходимо собирать данные о ботах и выполнять динамический анализ, прежде чем предпринимать какие-либо действия. Такие цели могут включать в себя обнаружение вредоносных регистраций, ставок, заявок на бонусы и т. д. Чтобы обеспечить тщательный анализ, службам безопасности может потребоваться объединить несколько источников данных как из внутренних, так и из внешних инструментов для анализа параметров трафика ботов.

Выполнение динамического анализа		
Проблема	**Решение**	**Результаты**
Букмекерская компания запустила маркетинговую кампанию по привлечению новых пользователей, предлагая вознаграждения за регистрацию. Вскоре после запуска они заметили, что боты совершают поддельные регистрации. У компании уже имелись некоторые инструменты внутренней аналитики, но они не давали полной картины поведения ботов.	Команда внедрила передовую систему **управления ботами** от Cloudflare с сигнатурами JA3 для генерации **необработанных журналов** всего интернет-трафика, поступающего на страницу регистрации. Они обогатили свои внутренние системы оценками ботов и сигнатурами JA3, что позволило им более четко идентифицировать ботов.	После тщательного анализа компания смогла отменить поддельные регистрации и избежать завышения статистики вновь приобретенных пользователей. Они внедрили регулярный анализ ботов с использованием сигнатур JA3 в свои лучшие методики.

Будьте на шаг впереди вредоносных ботов

Cloudflare Bot Management (Управление ботами)

Простое развертывание
Отсутствие необходимости в сложной настройке или техническом обслуживании

Низкая задержка
Средняя задержка < 0,3 мс

Богатая аналитика
Сопоставляйте журналы трафика с другими источниками данных, такими как SIEM или инструменты бизнес-аналитики (BI).

Точные элементы управления
Настраивайте правила, используйте визуальный конструктор правил или создавайте свои собственные правила сопоставления с шаблоном

Блокируйте вредоносные боты до того, как они нанесут вред вашему бизнесу

Боты совершенствуются с каждым днем. По мере того как подходы злоумышленников становятся все более изощренными, обнаружению и блокированию ботов становятся свойственны определенные ограничения. Современным компаниям необходимо постоянно корректировать свои стратегии, чтобы справиться с переоснащением злоумышленников, достигая при этом надлежащего баланса между надежной безопасностью и минимизацией помех для пользователей.

Какую бы стратегию вы ни выбрали, убедитесь, что у вашего партнера есть гибкий набор инструментов для эффективного управления ботами. Чтобы узнать больше о том, как Cloudflare может помочь вам решить проблемы с ботами, свяжитесь с нами для индивидуальной оценки.

Интеллектуальное решение, которому вы можете доверять

Cloudflare проксирует около 20 % всего глобального интернет-трафика, что обеспечивает получение обширной аналитики в режиме реального времени о поведении вредоносных ботов в сети Cloudflare.
Кроме того, Cloudflare работает с несколькими партнерами, которые обмениваются аналитическими сведениями об украденных учетных данных для входа, что упрощает обнаружение попыток захвата учетной записи до того, как эти попытки приведут к взлому.

Начните ваш путь к более быстрой, надежной и безопасной сети

Запросить консультацию

Не готовы к своей оценке?

Узнайте еще больше о Cloudflare