РЕШЕНИЕ ДЛЯ ЗАЩИТЫ ОТ БОТОВ

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

Group-IB Fraud Hunting Platform / Preventive Proxy

GROUP-IB FRAUD HUNTING PLATFORM

Система проактивной защиты цифровой личности и предотвращения мошенничества в режиме реального времени. Решение защищает пользователей мобильных приложений и веб-порталов финансовых организаций, государственных учреждений, интернет-магазинов и других онлайн-сервисов.

В рамках системы реализовано блокирование вредоносных ботов на онлайн-ресурсах заказчика.

Принцип выявления бот-активности основан на анализе поведения пользователя и окружения, в котором работает приложение.

Виды и последствия бот-атак, от которых защищает решение Group-IB:

Скрапинг

Технология получения данных путем извлечения их со страниц веб-ресурсов

Брутфорс

Взлом учетных записей и получение доступа к данным путем перебора паролей

Нежелательные расходы

Издержки на обработку запросов от ботов: СМС-рассылки пользователям, оплата дополнительных мощностей

Кража аккаунтов

Автоматический перебор скомпрометированных пар логинов/адресов почты пользователей и паролей, чтобы получить несанкционированный доступ к их учетным записям

Бот-активность с использованием мобильного API

Сбор данных и совершение мошеннических действий через мобильный канал

Отказ в обслуживании

Перегрузка запросами всего ресурса или его составляющих в результате бот-активности

Несанкционированное использование API

Прямые обращения к программному интерфейсу или его использование из сторонних или поддельных мобильных приложений

Использование средств автоматизации

Selenium, PhantomJS и т.д. — инструменты для автоматизации действий пользователей

Технологии работы защиты от ботов Group-IB

Кроме проверки заголовков и частотных характеристик запросов к серверам заказчика, решение дополнительно:

1

Анализирует действия пользователя, характеристики которых в случае работы бота будут отсутствовать или отличаться от человеческих (прямолинейность траектории мышки, программные клики и т.п.)

2

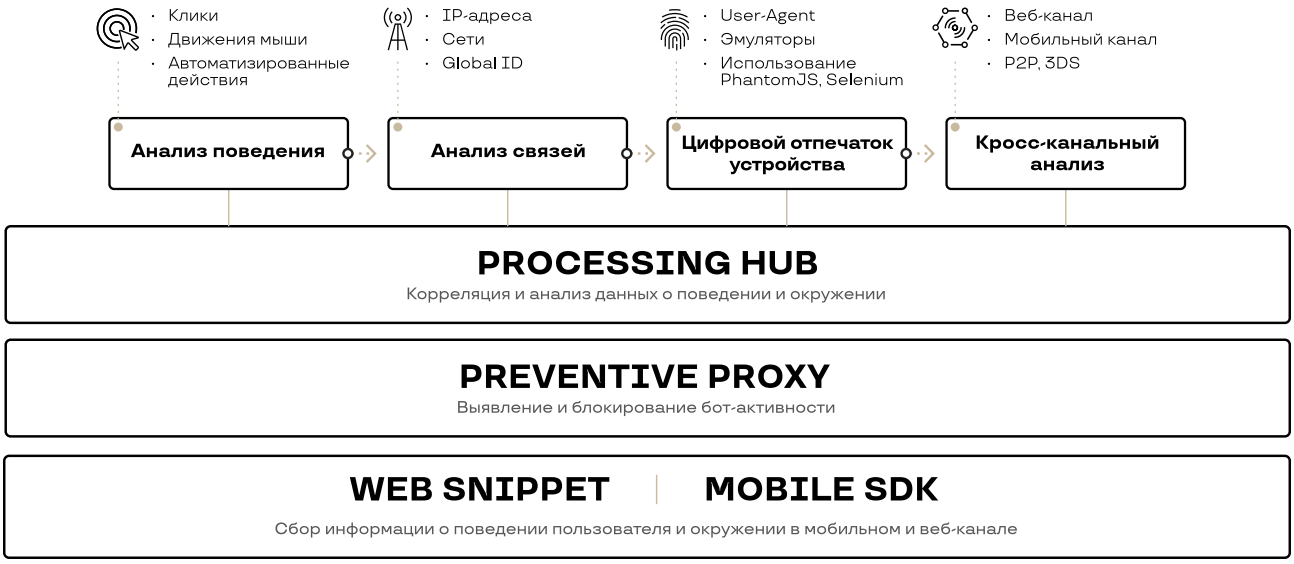
Собирает параметры браузера, приложения и устройства, характеристики которых в случае работы бота будут отсутствовать или отличаться от реальных (при использовании PhantomJS, Selenium, эмулятора мобильного устройства и т.п.)

3

Защищает параметры реальной пользовательской сессии от повторного использования ботами благодаря запатентованной технологии защиты

Состав и принцип работы защиты от ботов Group-IB

Group-IB Fraud Hunting Platform состоит из нескольких функциональных блоков:



Web Snippet

С момента загрузки первой страницы веб-ресурса передает в Processing Hub системы поведенческие характеристики пользователя и окружения, в котором работает веб-приложение.

Mobile SDK

Работает аналогично Web Snippet в составе мобильного приложения.

Preventive Proxy

Проверяет наличие, корректность и уникальность файлов cookie на запросах с устройства пользователя и на их основе принимает решение о наличии бот-активности или мошенничества.

Processing Hub

В ответ на полученные данные каждый раз формирует новый серверный файл cookie с вердиктом о наличии признаков бот-активности. Для каждого запроса из мобильного или веб-приложения Mobile SDK или Web Snippet дополнительно формируют и передают уникальный клиентский файл cookie на базе серверного.

В зависимости от вердикта и настроек Preventive Proxy может:

помечать запросы дополнительными HTTP-заголовками для последующей их обработки на серверах защищаемого приложения или интеграции с другими системами защиты информации.

пропускать запросы из доверенных источников или от легитимных ботов (поисковых систем и т.п.).

заблокировать или перенаправить на другую страницу.

Такой подход позволяет включать дополнительную проверку только для подозрительных запросов: от ботов или в случае ложных срабатываний защиты от них (по статистике их меньше 1%).

Ключевые преимущества

Непрерывный анализ сессии для выявления «умных» ботов, имитирующих поведение человека, включая отслеживание программных кликов, вставки данных, автоматизированных переходов по страницам

Противодействие продвинутым ботам, включая выявление эмуляторов устройств, анонимайзеров и средств автоматизации, за счет анализа поведения пользователя и окружения

Кросс-канальная защита API для мобильных и веб-приложений за счет противодействия перехвату и подмене данных в запросах к приложению

Унифицированная защита как мобильного, так и веб-приложения, которые могут использовать общий API

Выявление других видов мошенничества, которые совершаются людьми, таким образом обеспечивая более полную защиту цифровой личности

Улучшение пользовательского опыта благодаря запуску дополнительных проверок только для подозрительных запросов (например, с помощью CAPTCHA)

Повышение защищенности API от различных средств анализа и пентестинга

Сохранение конверсии за счет блокировки вредоносных запросов, а не IP-адресов

Гибкие варианты интеграции в облаке или в периметре клиента

Точное обнаружение и предотвращение атак за счет использования интегрированных данных о киберпреступниках, вредоносных программах, IP-адресах злоумышленников и скомпрометированных данных, полученные от Group-IB Threat Intelligence, Лаборатории компьютерной криминалистики и с помощью обезличенной обратной связи от клиентов

Защита от бот-активности не только в начале сессии работы пользователя, а на всем ее протяжении. Попытка переиспользовать наши токены доступа или ваш сессионный файл cookie не приведут к желаемому результату

Внедрение защиты от ботов Group-IB

Для работы защиты от ботов понадобится внедрить Web Snippet (для веб-портала) или Mobile SDK (для мобильного приложения) системы Group-IB Fraud Hunting Platform.

Preventive Proxy можно внедрить в инфраструктуру приложения или в облако Group-IB и настроить проксирование запросов через Preventive Proxy или модуль auth-request в NGINX.

Варианты поставки:

- Docker-контейнер
- Бинарный исполняемый файл
- Облако Group-IB

Обработка трафика возможна через:

- проксирование запросов внутри Preventive Proxy
- разметку с помощью auth-request в NGINX

Технические требования модуля Preventive Proxy

Для нагрузки в 20–30 тыс. запросов/с (исключая статический контент) минимальные ресурсы сервера.

Для минимизации времени обработки запросы на статический контент можно перенаправить через прокси-модуль в инфраструктуре приложения.

CPU	4 ядра, 2 потока на каждое ядро
RAM	8 Гб