Ежемесячный объем мобильного трафика во всем мире

1 эксабайт = 1 млрд гигабайт

2015	2016	2021[1]
4,4 эксабайт	7,2 эксабайт	49 эксабайт

До 15%

всего трафика в адрес мобильного API — из нелегитимных источников[2]

АНТИБОТ-ЗАЩИТА ДЛЯ МОБИЛЬНЫХ И ВЕБ-ПРИЛОЖЕНИЙ
КОМПЛЕКСНОЕ РЕШЕНИЕ APPROOV И PT APPLICATION FIREWALL

МОБИЛЬНЫЙ API ВАШЕГО ПРИЛОЖЕНИЯ — СЛАБОЕ ЗВЕНО?

Большая часть существующих мобильных приложений обращается напрямую к серверам разработчиков через интерфейс API. Извлечение из оригинального приложения информации об API и ключей доступа к нему не составляет большого труда. Это позволяет злоумышленникам свободно манипулировать запросами к API и автоматизировать атаки на приложение.

Целью подобных атак могут быть кража данных, мошеннические действия с учетными записями, платежными картами и программами лояльности, подбор паролей и спам, а также манипуляции с заказами в приложениях, предоставляющих товары и услуги, для исчерпания запасов или получения преимуществ перед другим пользователями. Эта угроза реальна: в среднем от 10 до 15% трафика в адрес мобильного API приходит из нелегитимных источников[2].

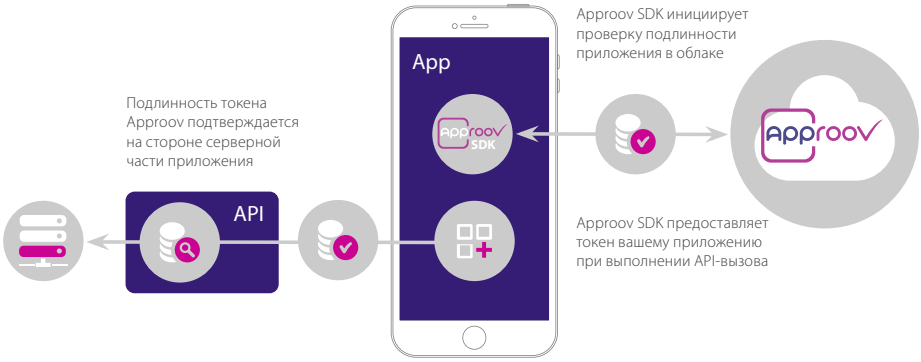
Нелегитимный трафик обычно создается автоматизированными скриптами (ботами), а также модифицированными или фальшивыми мобильными приложениями. Ситуация усугубляется тем, что межсетевые экраны уровня веб-приложений и API-шлюзы не распознают его как «плохой» — ведь боты используют корректные протоколы API, ключи и даже учетные данные пользователей. Последствия такой атаки могут быть катастрофическими:

- материальный ущерб в результате кражи данных конкурентами, утечки личных данных, неконтролируемого доступа к товарам или услугам;
- ущерб репутации компании в результате хищения или фальсификации учетных записей, а также ухудшения качества взаимодействия с пользователями;
- рост затрат на облачные сервисы или повышение нагрузки на серверы из-за обработки дополнительного нелегитимного трафика.

ЗАЩИТИТЕСЬ ОТ БОТОВ С ПОМОЩЬЮ APPROOV И PT APPLICATION FIREWALL

Approov — антибот-решение для мобильных приложений, разработанное компанией CriticalBlue, экспертами по динамическому анализу программного обеспечения. Оно аутентифицирует программное обеспечение, совершающее вызовы к мобильным API, и таким образом помогает:

1) блокировать трафик, генерируемый ботами (без мобильных приложений);
2) блокировать трафик от фальшивых или взломанных приложений.



ПРИНЦИП РАБОТЫ

Облачный сервис Approov проверяет каждое загруженное приложение на подлинность. Проверку автоматически инициирует SDK, который отправляет облачному сервису запрос на генерацию уникального токена, основанного на общем секрете и ограниченного по времени действия. SDK передает этот токен приложению для использования в API-вызовах. Проверяя подлинность токена с помощью общего секрета, ваши серверы (или PT AF) могут легко отличить «хороший» трафик, идущий от подлинных приложений, и блокировать нелегитимный.

Из Approov загружается общий секрет для проверки подлинности токена. Проверку токена на основе этого секрета вам необходимо добавить в серверный код. Этот шаг можно пропустить, развернув предварительно интегрированное решение PT Application Firewall (PT AF), которое будет выполнять проверку. Важно, что секрет не хранится в приложении, поэтому его нельзя оттуда украсть.

Approov легко развертывается и не снижает качество взаимодействия с конечным пользователем. Просто скачайте SDK, интегрируйте его в исходный код приложения и регистрируйте каждый релиз в Approov до его публикации в магазинах приложений.

Approov Authenticating Mobile Apps

1 statista.com/statistics/271405/global-mobile-data-traffic-forecast/
2 По данным клиентов CriticalBlue.

ПРЕИМУЩЕСТВА APPROOV

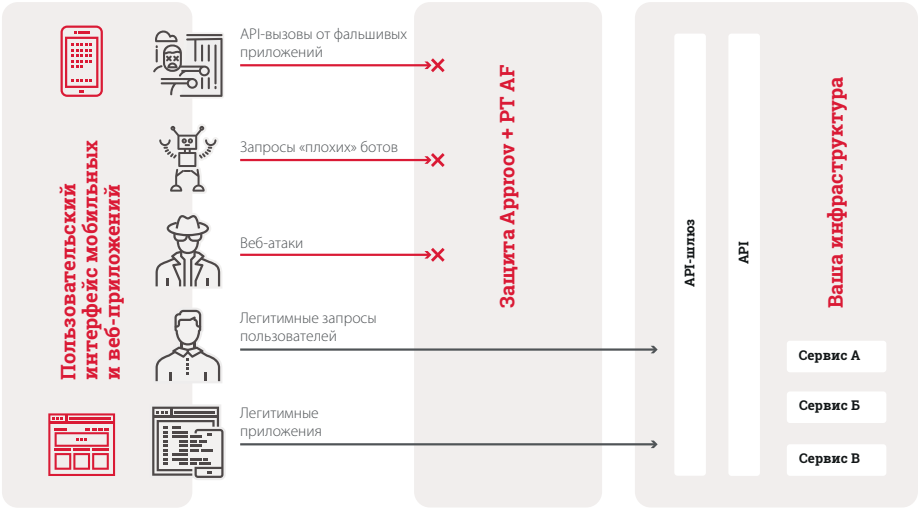
+ **Защита прибыли.** Данные, которыми вы дорожите, будут недоступны для конкурентов и злоумышленников.
+ **Защита репутации и данных клиентов.** Качество взаимодействия с пользователем и уровень доверия снижаются, когда клиенты сталкиваются с фишингом, рассылкой спама или хищением данных. Защитите себя от потери клиентов и штрафов со стороны регуляторов.
+ **Прозрачность.** Получайте информацию не только о том, кто взаимодействует с вашим сервером, но и каким образом.
+ **Сокращение затрат.** Уменьшайте нагрузку на ваши локальные или облачные серверы, блокируя нелегитимный трафик.

ОБЕСПЕЧЬТЕ ЗАЩИТУ ВСЕХ КАНАЛОВ ЭЛЕКТРОННОГО БИЗНЕСА

Наряду с мобильными приложениями ваши веб-приложения также нуждаются в эффективной интеллектуальной защите от автоматизированных атак. Комплексное решение, объединяющее Approov и PT Application Firewall, способно ее обеспечить.

Хотя боты решают множество полезных задач, хакеры с энтузиазмом используют их для мошеннических действий в интернете. Большая часть интернет-трафика сегодня генерируется автоматически, а боты становятся не только более многочисленными, но и более сложными, и их все сложнее обнаруживать. От простых автоматизированных скриптов, которые было легко заметить из-за отсутствия пользовательских cookies или JavaScript, они прошли путь до имитации браузеров и теперь могут подражать поведению человека или скрываться за легитимными пользовательскими сессиями.

Чтобы блокировать нелегитимный трафик незаметно для реальных клиентов, необходимы инструменты, сочетающие в себе разные методы обнаружения, в основе которых лежат технологии поведенческого анализа. Наилучшим вариантом является межсетевой экран уровня веб-приложений (WAF), который способен обнаруживать и блокировать нелегитимный трафик всех типов.



Комплексная интеллектуальная защита ваших мобильных и веб-каналов

+ Только легитимные пользователи и приложения
+ Отсутствие негативного воздействия на реальных пользователей и легитимные приложения
+ Постоянное обучение на реальном трафике и учет контекста приложений для наибольшей скорости обнаружения

PT APPLICATION FIREWALL: УМНЕЕ САМЫХ УМНЫХ БОТОВ

PT AF не только предоставляет быстрый, предварительно интегрированный способ развертывания Approov, но и является универсальным ответом на вопросы обеспечения безопасности самых разных приложений — от веб-порталов до систем управления ресурсами предприятия и мобильных приложений.

PT AF сочетает сигнатурный и эвристический методы анализа, что позволяет ему блокировать все типы атак на приложения и на связанные с ними веб-технологии, не воздействуя на деятельность легитимных ботов. Благодаря передовым возможностям PT AF Positive Technologies признана визионером в магическом квадранте Gartner 2017 по безопасности веб-приложений — уже третий год подряд.

PT AF может быть развернут как аппаратное решение или виртуальное устройство, полностью готов к использованию в облаке, в том числе через Microsoft Azure.

Чтобы узнать больше о функциональности и преимуществах PT AF, скачайте обзор решения.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays