ОТСЛЕЖИВАНИЕ ТРАФИКА БОТОВ И ЗАЩИТА ОТ БОТ-АТАК В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

ПРЕДОТВРАЩЕНИЕ АВТОМАТИЗИРОВАННЫХ АТАК НА ВЕБ-САЙТЫ, МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ И API

За последнее время угроза автоматизированных атак затронула почти каждую индустрию. Конкуренты и мошенники запускают человекоподобные боты, имитирующие действия реального пользователя, для атак на веб-сайты, мобильные приложения и API, таких как захват учетных записей, мошенничество с подарочными картами и цифровой рекламой, веб-скрейпинг и спам. Мошенники используют тысячи ботов, совершая крупномасштабные распределенные атаки на интернет-ресурсы. Часто это медленные маломощные атаки (так называемые атаки low and slow), которые проходят незаметно для обычных систем защиты. Автоматизированные атаки негативно влияют на впечатления клиентов от использования ресурса, портят репутацию компании, искажают аналитику и приносят убытки.

Решение для защиты от ботов Radware Bot Manager в режиме реального времени обнаруживает и блокирует сложные человекоподобные боты без нарушения качества сервиса и работы реальных пользователей. В нашем механизме обнаружения ботов использована фирменная технология глубокого анализа поведения на основе намерений (IDBA), позволяющая понять намерение посетителей и отфильтровать недопустимый трафик вредоносных ботов. Мы собираем более 250 параметров, включая особенности поведения при просмотре страниц, движения мыши, нажатия клавиш и перемещения по URL-адресам в браузере, а затем применяем проприетарные алгоритмы для создания уникальных цифровых отпечатков каждого пользователя. Наша база цифровых отпечатков ботов (collective bot intelligence) содержит сигнатуры ботов, собранные с более чем 80 000 интернет-ресурсов наших клиентов, и позволяет предупреждать проникновение вредоносных ботов на ваши интернет-площадки.

Мы защищаем вас от следующих атак:

Захват учетных записей
Злоумышленники используют атаки с заполнением учетными данными (credential stuffing) и взлом методом перебора (brute force attack) для получения незаконного доступа к учетным записям клиентов.

Мошенничество с подарочными картами
Мошенники используют боты для взлома подарочных карт, чтобы определить номера купонов и коды ваучеров.

DDoS-атаки на приложения
DDoS-атаки на приложения замедляют работу веб-приложений из-за истощения системных ресурсов, перегрузки партнерских API, учетных баз данных и других важных ресурсов.

Скрейпинг цен
Конкуренты запускают боты на ваши веб-сайты для кражи информации о ценах и переманивания ваших покупателей.

Веб-скрейпинг
Мошенники и агрегаторы с помощью ботов извлекают данные и незаконно используют украденный контент на сайтах-призраках.

Мошенничество с цифровой рекламой
С помощью вредоносных ботов накручиваются просмотры рекламы и клики на рекламных площадках и в их мобильных приложениях.

Искажение аналитики
Автоматизированный трафик на интернет-ресурсы искажает метрики, что может привести к принятию ошибочных решений.

Спам
Вредоносные боты наводняют интернет-магазины и различные общественные форумы спамом, ссылками, комментариями и поддельными регистрациями.

Основные характеристики

Глубокий анализ поведения на основе намерений (IDBA)

Многие искусно организованные атаки ботов либо радикально распределены, либо достаточно медленные и маломощные (так называемые low and slow), чтобы их трафик укладывался в пределы допустимых значений правил средств безопасности. Radware использует фирменную технологию глубокого анализа поведения на основе намерений (IDBA), чтобы распознать предназначение сложного машинного трафика. IDBA анализирует поведение на более высоком уровне выявления намерений, в отличие от распространенных методов поверхностного анализа на основе взаимодействия. Понимание намерения позволяет IDBA более точно распознавать ботов, которые умеют хорошо имитировать действия человека. IDBA базируется на результатах наших исследований в сфере полуконтролируемого машинного обучения и новейших методов глубокого обучения.

Возможность разных способов обработки бот-трафика

Агрегаторы и конкуренты постоянно атакуют веб-ресурсы с целью похитить цены, контент и другую важную для бизнеса информацию. Решение Radware Bot Manager позволяет использовать настраиваемые действия для реагирования на атаку с учетом сигнатур/типов ботов. Вы можете перехитрить конкурентов, передавая запущенным ими ботам искаженные цены и информацию о товарах. Для обнаружения машинного трафика также могут применяться проверки, например CAPTCHA. Ответы, полученные в ходе проверки, помогают нам создать замкнутую систему обратной связи и свести к минимуму количество ложных срабатываний. Наше решение для защиты от ботов позволяет рекламным площадкам показывать объявления только реальным пользователям и блокировать недопустимый машинный трафик еще до загрузки страниц.

Прозрачные отчеты и комплексная аналитика

Прозрачные отчеты о трафике помогут вам построить доверительные отношения с коллегами и партнерами. Детализированная классификация ботов, например поисковых роботов и вредоносных ботов, позволит вам эффективно управлять машинным трафиком. Прозрачная аналитика и отчеты позволяют отслеживать веб-трафик и получать детальную картину поведения ботов на ваших интернет-ресурсах. Radware предоставляет средства комплексного анализа трафика ботов, его источников и URL. Одно из ключевых преимуществ механизма обнаружения ботов — это подробные и прозрачные отчеты. Отчеты особенно полезны для некоторых видов автоматизированных угроз, таких как мошенничество с цифровой рекламой. Панель аналитики показывает характерное поведение пользователей на вашем сайте. Наше решение для защиты от ботов можно легко интегрировать с ведущими аналитическими платформами, включая Google Analytics и Adobe Analytics.

Простая интеграция

Radware Bot Manager обеспечивает простые и гибкие варианты развертывания с учетом задач вашего бизнеса. Вы можете интегрировать тег JavaScript, облачные коннекторы или плагин веб-сервера в свою инфраструктуру за считаные минуты. Или можете выбрать наше виртуальное устройство. Если вам не нужно интегрировать наше решение во все веб-приложение, это можно сделать только для определенных разделов веб-сайта.

Интеграция без перенаправления DNS

Перенаправление DNS представляет риски для критически важных корпоративных приложений. Если DNS не работает, то и ваш бизнес тоже. Решение Radware Bot Manager основано на API и не требует перенаправления DNS. В результате вы получаете независимость от внешних DNS и полный контроль над вашими мобильными и веб-приложениями и API.

Точность и масштабируемость

Попытки обнаружения сложных ботов на основе поверхностных характеристик взаимодействия приводят к большому количеству ложных срабатываний. Наша технология глубокого анализа поведения на основе намерений помогает обнаруживать сложных ботов, имитирующих действия человека, и не вызывает ложных срабатываний. Radware гарантирует, что инструмент никак не нарушит работу вашего веб-сайта и пользователей. Мы применяем передовые технологии, такие как оркестрация контейнеров Kubernetes и брокер Kafka, чтобы масштабировать производительность во время пиковой нагрузки.

Принцип работы Radware Bot Manager

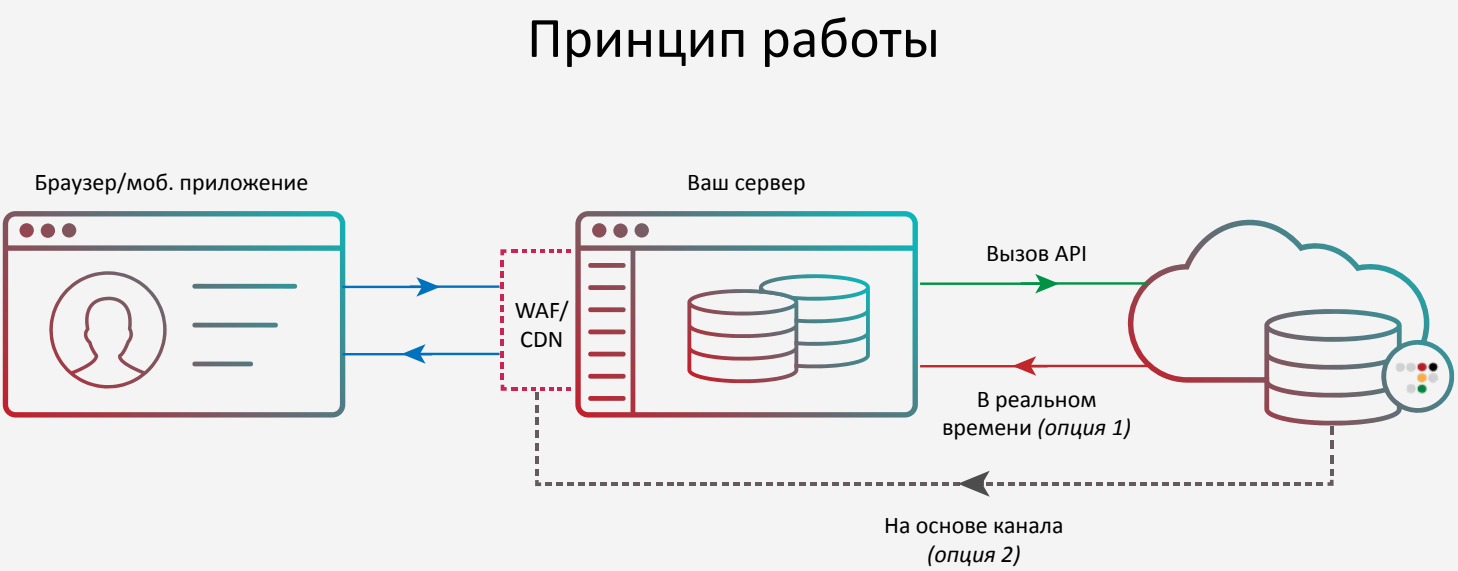

Рисунок 1. Диаграмма Radware Bot Manager

Анализ трафика

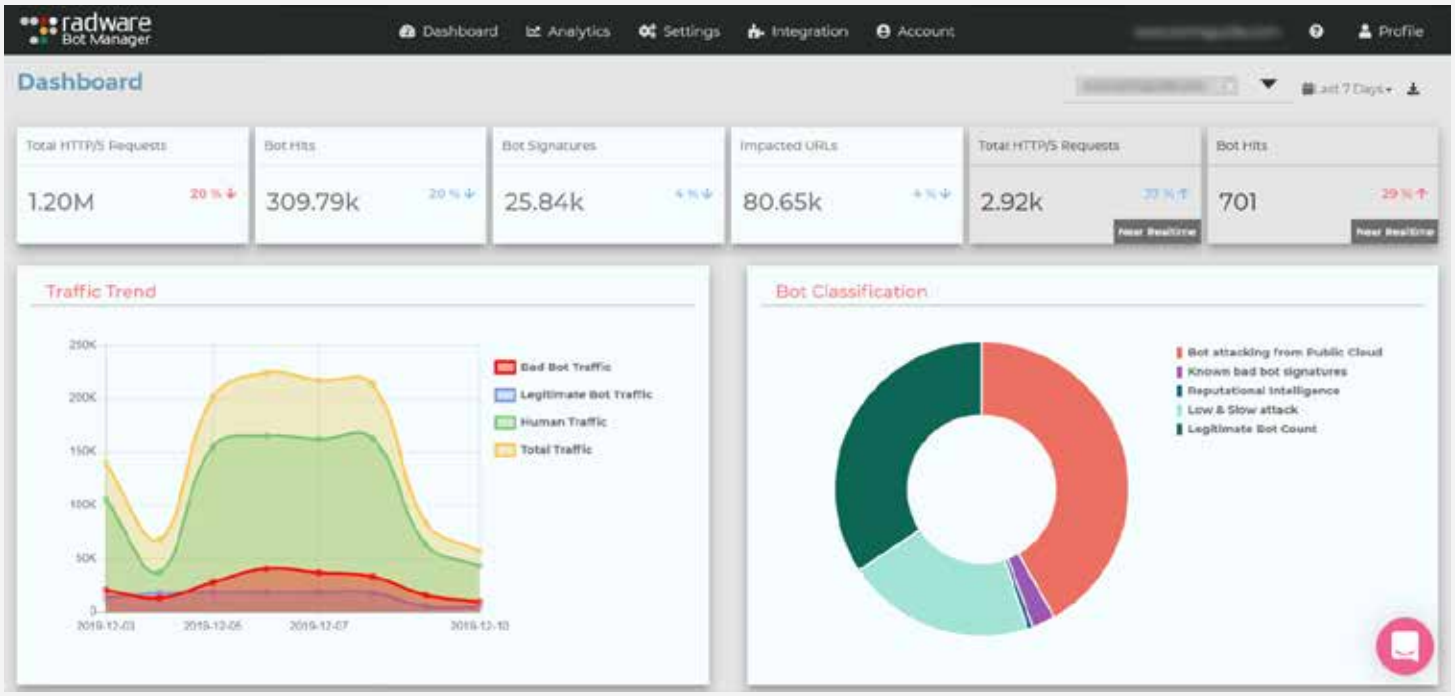

Рисунок 2. Диаграмма анализа трафика в Radware Bot Manager

О компании Radware

Компания Radware® (NASDAQ: RDWR), ведущий поставщик решений для обеспечения кибербезопасности и доставки приложений, приобрела ShieldSquare в марте 2019 года. ShieldSquare теперь называется Radware Bot Manager.

Компания Radware® (NASDAQ: RDWR) — мировой лидер в области создания решений для обеспечения кибербезопасности и доставки приложений для физических, облачных и программно-определяемых центров обработки данных. Наши отмеченные наградами решения защищают цифровую среду, предоставляя предприятиям по всему миру сервисы для защиты инфраструктуры, приложений и ИТ-ресурсов. Решения Radware позволяют клиентам более чем 12 500 предприятий и операторов связи по всему миру быстро адаптироваться к изменениям на рынке, поддерживать непрерывность бизнеса, повышать производительность и снижать затраты. Дополнительную информацию см. на www.radware.com.

Radware призывает вас присоединиться к нашему сообществу и подписаться на наши ресурсы: Facebook, LinkedIn, Radware Blog, Twitter, YouTube, Radware Mobile для iOS и Android и наш центр безопасности DDoSWarriors.com, где вы найдете детальный анализ инструментов, тенденций и угроз DDoS-атак.