radware

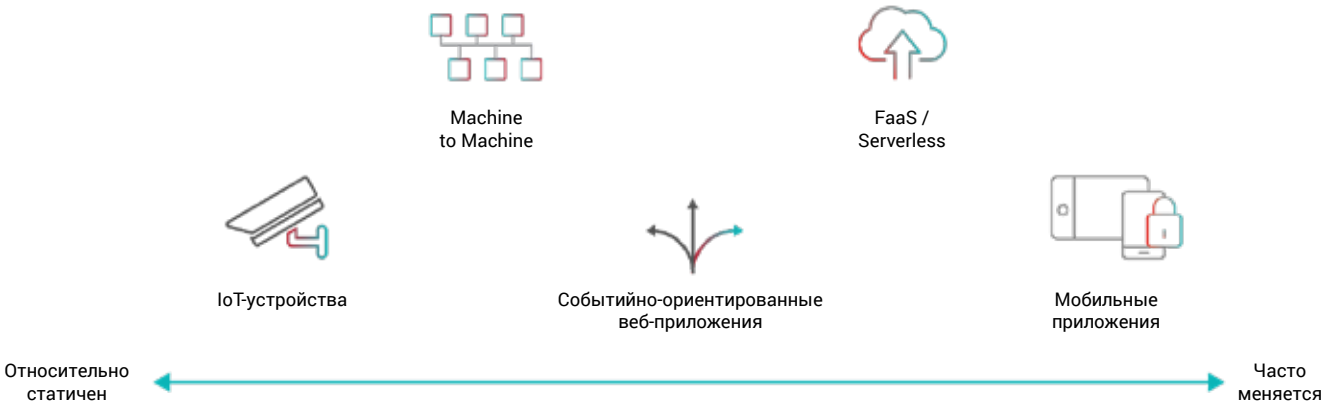
Технологии Radware Bot Manager для защиты API

ИНФОРМАЦИОННЫЙ ДОКУМЕНТ

ОГЛАВЛЕНИЕ

Введение. Актуальные проблемы безопасности API

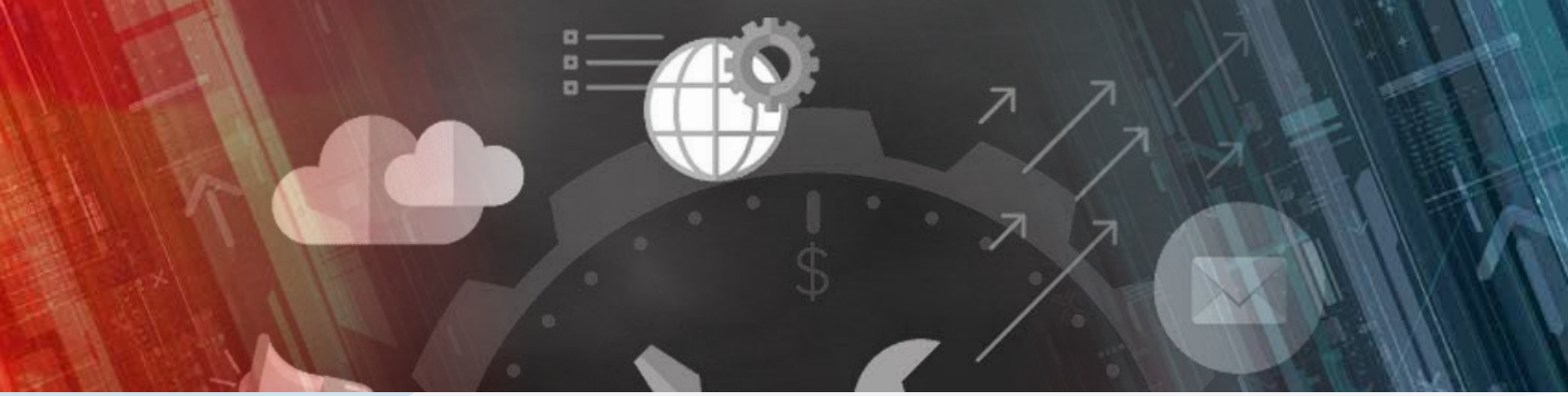
Интерфейсы прикладного программирования (API) появились для обеспечения взаимодействия систем, сетей и приложений. Существуют специальные протоколы передачи данных API, и от них зависят многие экосистемы и архитектуры – от смартфонов до ячеистых сетей и операционных технологий (OT). Без API не обходятся инженеры DevOps, облачные архитекторы и ИТ-отделы. С началом массового внедрения API появилась необходимость защищать их от любых потенциальных вторжений и применения в преступных целях.
К сожалению, несмотря на массовое применение, интерфейсы API плохо защищены от автоматизированных атак. Личные сведения (PII), реквизиты банковских карт и критически важные для бизнеса сервисы находятся под угрозой из-за атак ботов на API.



Автоматизированные атаки на API и пробелы в системе безопасности

Количество атак ботов на API стремительно растет. За первую половину 2020 года их активность повысилась на 30% по сравнению с 2019 годом. Эти боты использовались для осуществления автоматизированных атак на API, включая захват учетных записей, атаки типа «отказ в обслуживании», использование похищенных платежных данных и атаки на исчерпание запасов склада онлайн-площадок (denial of inventory). Защита API от автоматизированных атак отличается от защиты мобильных и веб-приложений, попросту потому что поведение, маршруты и индикаторы атакующих ботов заметно отличаются.

API предназначены для ускорения бизнес-процессов и, учитывая разрешенный доступ для большей части трафика API, необходимо различать автоматизированный трафик с хорошими и вредоносными намерениями. В большинстве решений для защиты от ботов модели машинного обучения построены на сборе данных из браузеров и внешних источников трафика для разделения трафика реальных пользователей и ботов. Чтобы распознать вредоносное намерение во время вызова API, необходим совершенно другой подход, поскольку человек здесь напрямую не участвует. Традиционные решения используют цифровой отпечаток устройств для обнаружения ботов, использующих вращающиеся (ротационные, rotating) IP-адреса или пользовательские агенты. Однако эта технология не подходит в случае межмашинного взаимодействия. Это один из недостатков, которые Radware устраняет с использованием своих специальных технологий защиты API.



Основные уязвимости API

1. Недостатки аутентификации

Многие API не проверяют статус аутентификации, если запрос приходит от зарегистрированного пользователя. Существуют различные методы использования этого недостатка, такие как перехват сеанса и агрегирование учетных записей, которые имитируют законные вызовы API. Злоумышленники также декомпилируют мобильные приложения, чтобы узнать, как вызываются API. Если ключи API встроены в приложение, возможен взлом API. Ключи API не следует использовать для аутентификации пользователей.

2. Отсутствие надежного шифрования

Многим API не хватает надежного шифрования между клиентом API и сервером. Злоумышленники используют эти уязвимости и осуществляют активное вмешательство в соединения – т.н атаки «злоумышленник в середине» (атака посредника, man-in-the-middle/MITM). Злоумышленники перехватывают незашифрованные или плохо защищенные API-транзакции для кражи конфиденциальных данных или искажения информации. Повсеместное использование мобильных устройств, облачных систем и шаблонов (паттернов) микросервисов дополнительно усложняет задачу обеспечения безопасности API, так как теперь для организации взаимодействия разнородных приложений используются многочисленные шлюзы. Шифрование данных, передаваемых по всем этим каналам, имеет первостепенное значение.

3. Уязвимость бизнес-логики

API уязвимы для злоупотреблений бизнес-логикой. Именно поэтому для противодействия ботам требуется специализированное решение, а механизм обнаружения ботов, который одновременно используется для мобильных и веб-приложений, может стать причиной многих ошибок, таких как ложное срабатывание и игнорирование тревожных сигналов.

4. Недостаточная безопасность конечных точек

Большинство IoT-устройств и инструментов микросервисов запрограммированы на взаимодействие с сервером по API-каналам. Эти устройства подтверждают свою подлинность на серверах API с помощью сертификатов клиентов. Хакеры пытаются получить контроль над API из конечной точки IoT. Если им это удается, они могут легко изменить порядок API, что приводит к утечке данных.

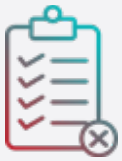
Типичные автоматизированные атаки на API

Захват учетных записей

Атаки с захватом учетных записей бывают двух видов: (1) взлом учетных записей (credential cracking ; (2) заполнение учетых данных (credential stuffing). Во время атаки с подбором учетных данных злоумышленники пытаются определить действительные учетные данные, вводя разные комбинации имени пользователя и (или) пароля. Во время атаки с заполнением учетными данными злоумышленники предпринимают попытку массового входа в систему, используя украденные учетные данные. В интерфейсах API киберпреступники пытаются получить прямой доступ к API или избежать процедуры идентификации устройства, чтобы захватить учетную запись.

Веб-скрейпинг

Сегодня многие компании имеют в штате специалистов по автоматическому сбору информации из Интернета или обращаются к сторонним профессионалам, чтобы получить преимущество перед конкурентами. Злоумышленники планируют атаку в несколько этапов, чтобы определить и использовать уязвимые места существующих систем. В частности, они запускают боты для сканирования уязвимостей API и используют недостаточно защищенные API для кражи конфиденциальной информации.



Исчерпание товаров/услуг на складе онлайн-площадки (Denial of Inventory)

Киберпреступники декомпилируют API, а затем используют человекоподобные боты, которые имитируют действия реального пользователя и добавляют товары в корзину. Эти боты отправляют запросы на конечную точку API, имитируя действия реального пользователя. Пока огромное количество ботов одновременно добавляют товары в корзину, повторяя процесс по истечении времени ожидания, реальные пользователи не могут совершать покупки.

DDoS-атаки на приложения

Прикладной уровень технологического стека напрямую влияет на взаимодействие с пользователем. Распределенные атаки типа «отказ в обслуживании» (DDoS) на уровне 7 создают угрозу для бизнес-процессов. Последствиями таких атак являются перегрузка API и низкая производительность сервисов. Атаки на уровне 7 также вызывают простои в случае распределенных и скоординированных DDoS-атак.

Непрерывность бизнеса с защитой API

Сейчас стало понятно, что использование API помогает повышать производительность, автоматизировать процессы и создавать идеальные конвейеры CI/CD. Наша задача состоит в том, чтобы найти такое решение для обеспечения безопасности, которое не будет вызывать сбоев и хорошо интегрируется в операционную среду. К сожалению, большинство традиционных решений не предназначены для обработки потоков API, потому что используют привычные сигнатуры и цифровые отпечатки для обнаружения автоматизированного трафика API. Данных о профиле пользователя недостаточно для защиты API. Чтобы предотвратить сложные автоматизированные атаки на API, необходимы инструменты защиты от ботов, использующие многоуровневые методы обнаружения и отслеживания трафика ботов, такие как статистический анализ коммуникации, прогнозирование маршрутов и контекстный механизм оценки. Такой подход обеспечивает минимальное количество ложных срабатываний, то есть минимальное количество случаев блокировки реальных пользователей. Кроме того, крайне важно различать и пропускать трафик полезных для бизнеса «хороших» ботов.

Инструменты защиты от ботов прежде всего и главным образом должны способствовать развитию бизнеса и не должны создавать «*шум*». Поэтому, в целях улучшения качества сервиса и работы пользователей, они должны быть оптимизированы для потоков вызовов API. В таком случае решение для защиты от ботов должно быть платформенно-независимым и интегрируемым в комплексную систему автоматизации.

Radware Bot Manager для защиты API
объединяет эти технологии, используя для предотвращения атак модуль быстрого реагирования (immediate response engine), детерминированный модуль (deterministic engine) и модуль машинного обучения. Все три модуля работают вместе, но главным для отражения автоматизированных атак является модуль быстрого реагирования. В следующем разделе мы разберем роль многоуровневой системы защиты в распознавании и отражении автоматизированных атак.

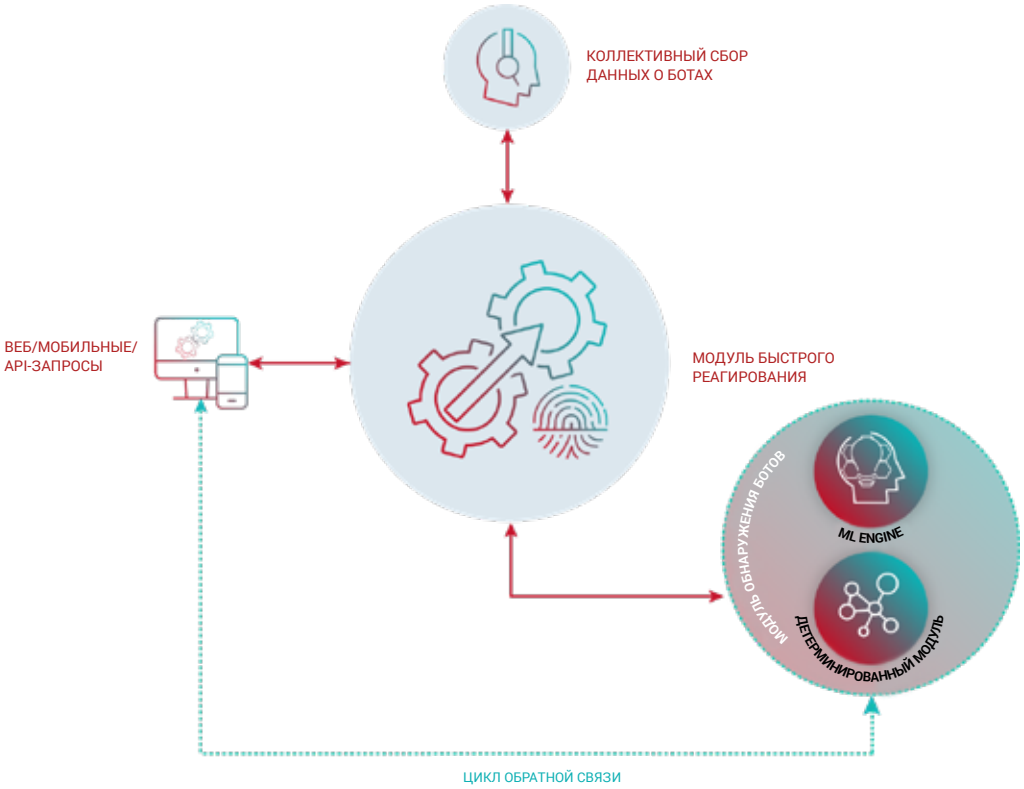


Рисунок 1. Radware Bot Manager: модуль обнаружения ботов

Модуль быстрого реагирования

Модуль быстрого реагирования отвечает на действия подозрительного посетителя сразу же при обнаружении активности, не связанной с человеком. В большинстве случаев он распознает бот при первой атаке. Полагаясь на работу детерминированного модуля и модуля машинного обучения, модуль быстрого реагирования распознает подозрительного пользователя, как только он заходит на сервер веб-приложения. Этот модуль работает совместно с модулем машинного обучения и детерминированным модулем для быстрого и эффективного реагирования на потенциальную угрозу. Модуль быстрого реагирования нацелен на прекращение активности бота при первой атаке. Как показано на рисунке 1, модуль быстрого реагирования распознает 70% вредоносных ботов при первой атаке.

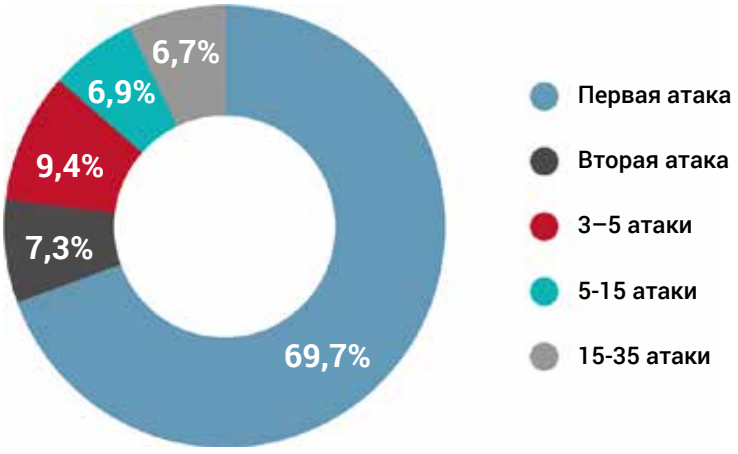


Рисунок 2. Боты, заблокированные модулем быстрого реагирования, — статистика распознавания

Модели машинного обучения

Модели машинного обучения — это основные компоненты для обнаружения и предотвращения сложных автоматизированных атак на API. Например, Radware Bot Manager для защиты API использует специально разработанные, проприетарные модели машинного обучения, такие как модуль контроля потоков API, модуль контекста вызова, анализ потоков аутентификации и глубокий анализ поведения на основе намерений. Модуль машинного обучения в Radware Bot Manager основан на позитивной модели безопасности. Он подстраивается под изменяющиеся шаблоны поведения ботов и гарантирует, что последующие запросы доступа будут немедленно отклонены. Далее мы подробно рассмотрим, как Radware Bot Manager использует модели машинного обучения для улучшения автоматического обнаружения и предотвращения атак.

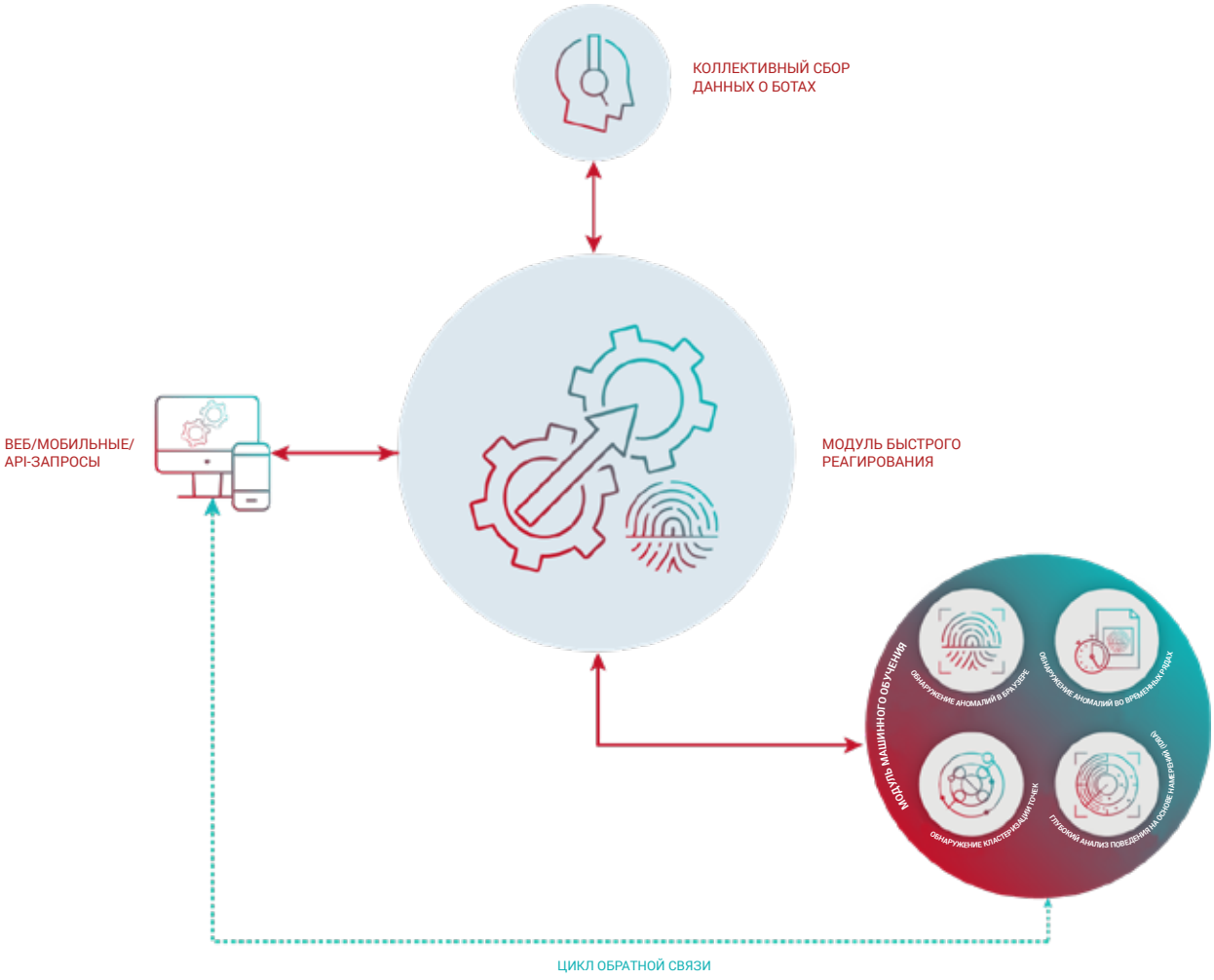


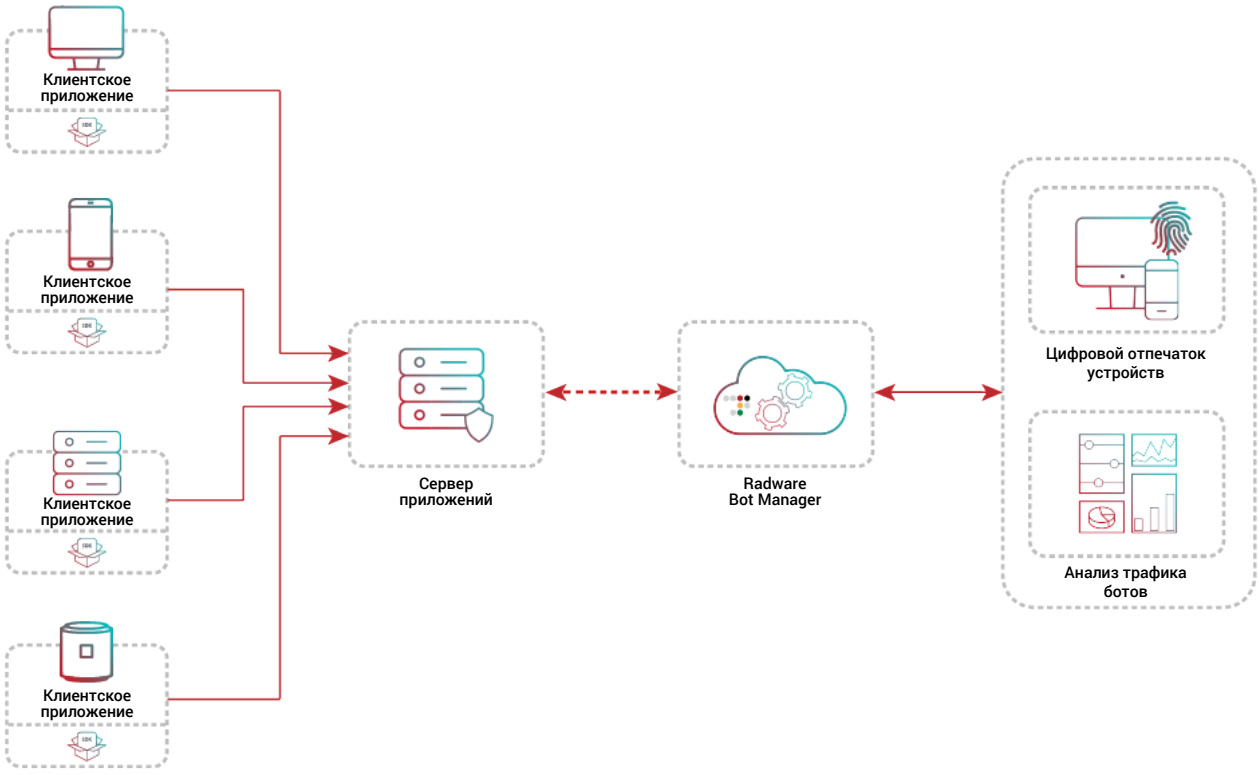
Рисунок 3. Radware Bot Manager: модуль машинного обучения

i. Контроль потока API — защита межмашинного взаимодействия и IoT

Обнаружение вредоносных действий, направленных на API, отличается от отслеживания вредоносного трафика мобильных и веб-приложений. В API необходимо различить «хорошие» вызовы API и «плохие» вызовы API. Решение, которое бы позволило распознавать вредоносные действия, должно идеально понимать особенности межмашинного взаимодействия и обнаруживать аномалии в поведении. Модуль контроля потока API в Radware Bot Manager основан на статистических моделях доступа к API, которые генерируются автоматически при изучении маршрутов доступа в течение определенного периода. Он основан на моделировании потока API между конечными точками API и ожидаемых вероятностях перехода между узлами. Как только модель готова, начинается анализ текущих маршрутов доступа с поиском подозрительной последовательности. В этом случае доступ блокируется. Этот модуль обеспечивает действенный способ идентификации подозрительных маршрутов доступа API и повышает общую безопасность API.

ii. Набор средств разработки (SDK) клиента API — защита API межмашинного взаимодействия (Machine to Machine, M2M)

SDK клиента для защиты API межмашинного взаимодействия — это еще один модуль обнаружения вредоносных вызовов API. Этот модуль собирает параметры API, такие как архитектура устройства, сведения о центральном процессоре и другие для разграничения подлинных и вредоносных вызововAPI. На этом этапе каждый API рассматривается как узел, и вероятный маршрут потока от одного узла к другому может быть представлен в виде арки. Поток с малой вероятностью блокируется. Этот модуль значительно помогает в распознавании вредоносных ботов, которые имитируют подлинные вызовы API на ваших интернет-ресурсах.



iii. Контекст вызовов — защита веб- и мобильных API

Вредоносного бота, нацеленного на API, можно распознать при помощи анализа контекста вызовов и последовательности действий, которые совершает пользователь. Многие боты пытаются обойти некоторые этапы, такие как вход в систему и навигация по сайту, перед доступом к API, чтобы как можно быстрее получить информацию. Radware анализирует API-трафик с точки зрения правильного контекста и запрещает доступ к API без предшествующих веб-транзакций или вызовов с мобильного устройства. Этот модуль позволяет отфильтровывать вредоносные вызовы API, как только они начинают коммуникацию.

iv. Анализ потока аутентификации — защита от захвата учетной записи для API

Модуль анализа аутентификации потока позволяет перехватывать ответ на запрос от API аутентификации. Модуль получает данные от API аутентификации и пересылает их модулю обнаружения ботов для анализа. Во время этого проверяются права доступа к ресурсам, обнаруживаются неудачные попытки входа в систему и блокируется источник атаки, генерирующий многочисленные неудачные попытки API входа. Анализ потока аутентификации особенно полезен для защиты API от сложных атак с захватом учетной записи (как с заполнением учетными данными (credential stuffing), так и с их подбором (credential cracking)).

v. Глубокий анализ поведения на основе намерений (IDBA, запатентованная технология)

Обычные системы защиты часто не замечают сложные, автоматизированные атаки, поскольку боты эволюционировали от базовых скриптов до крупномасштабных распределенных ботов, имитирующих поведение человека для обхода механизмов обнаружения. Технология глубокого анализа поведения на основе намерений выполняет поведенческий анализ на более глубоком уровне выделения намерений, в отличие от обычно используемого поверхностного поведенческого анализа, основанного на взаимодействии. Например, захват учетной записи — это пример намерения, а «указатель мыши, движущийся по прямой линии», — пример взаимодействия. Чтобы зафиксировать путь посетителя по веб-ресурсу, анализируются последовательность пройденных URL-адресов, источники перехода и время, проведенное на каждой странице. Анализ намерения обеспечивает существенно более высокий уровень точности при обнаружении продвинутых ботов с возможностями имитации поведения человека. Технология глубокого анализа поведения на основе намерений базируется на результатах наших исследований в сфере полуконтролируемого обучения (semi-supervised).

Дополнительные механизмы защиты в Radware Bot Manager

Модуль детерминированного моделирования

Одна из проблем, с которыми сталкиваются разработчики средств управления ботами, — большой объем входящего трафика. Обработка всего трафика с помощью модуля машинного обучения с последующим анализом поведения увеличивает общее время реагирования на атаку. Когда организация атакована, скорость реакции играет определяющее значение. Модуль детерминированного моделирования применяется в качестве основного модуля вместе с модулем быстрого реагирования. Это уменьшает общее время отклика на атаку и помогает обнаруживать большинство вредоносных ботов при первой атаке. В основе работы модуля детерминированного моделирования лежит анализ данных. Он руководствуется детерминированными правилами и анализирует HTTP-заголовки и данные JS, собранные с устройства конечного пользователя, для обнаружения сложного злонамеренного поведения.

Проверки целостности

Многие API открыты для сторонних приложений за пределами организации. Кибер-преступники используют открытые API для кражи персональных (PII) и других критически важных для бизнеса данных. Для организаций, собирающих личные и финансовые данные, любая форма раскрытия может привести к потере доходов и репутации. Radware выполняет расширенные проверки целостности для выявления ботов, эмуляторов и попыток декомпилировать SDK мобильных приложений или получить доступ к открытым API. Решение также использует механизм ограничения скорости (rate limiting) на основе нескольких параметров, чтобы предотвратить циклический выпуск и распределение токенов.

Накопленные сведения о ботах (Collective Bot Intelligence)

Уникальная база цифровых отпечатков ботов и пользователей, созданная на основе собранных сведений об угрозах ботов из нашей обширной клиентской базы по всему миру и вертикалям, способствует повышению точности и надежности системы обнаружения ботов. Наш центральный модуль обнаружения ботов использует накопленные сведения о ботах для отслеживания и предупреждения о ботах, а также для упреждающей защиты API.

Преимущества

Машинное обучение

Гибкое развертывание

Полная защита

Детальная визуализация

Заключение

Сегодня злоумышленники умеют обходить средства защиты, располагая большим набором инструментов для автоматизированных атак. Они используют продвинутые инструменты, наборы эксплойтов и методы введения в заблуждение для программирования ботов на имитацию действий человека и обход системы безопасности. Злоумышленники постоянно совершенствуют методы атаки и повышают эффективность ботов.
С развитием API появился целый арсенал сложных атак, которые используют уязвимости неконтролируемых потоков трафика и неконтролируемого доступа к конфиденциальным данным. Площадь атак все время расширяется, и организации пытаются справиться с хаосом. Выиграть войну с киберпреступниками и бесчисленным количеством запускаемых ими ботов с помощью универсального решения безопасности невозможно. Организациям требуется специализированный инструмент для противодействия ботам, такой как Radware Bot Manager. Это решение сочетает в себе модели машинного обучения, настроенные для обнаружения и отражения атак сложных ботов для защиты веб-сайтов, мобильных приложений и API.

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. Отмеченный наградами портфель решений этой компании защищает цифровое взаимодействие, предоставляя предприятиям по всему миру сервисы, обеспечивающие защиту и доступность инфраструктур, приложений и корпоративных ИТ-ресурсов. Решения Radware позволяют клиентам более чем 12 500 предприятий и операторов связи по всему миру быстро адаптироваться к рыночным вызовам, поддерживать непрерывность бизнеса и достигать максимальной производительности при одновременном снижении затрат. Для получения дополнительной информации, пожалуйста, посетите www.radware.com

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

radware

www.radware.com