

КАК ЗАЩИТИТЬ API ОТ КИБЕРАТАК БОТОВ

Широкое распространение мобильных устройств и устройств IoT, появление «бессерверных» архитектур, размещенных в общедоступных облаках, и рост зависимости от межмашинного взаимодействия (machine-to-machine) порождают изменения в архитектурах современных приложений. Прикладные программные интерфейсы (API) появились как связующее звено для взаимодействия между различными архитектурами приложений. API позволяют быстрее интегрировать и быстрее развертывать новые сервисы. Кроме того, для DevOps требуется сквозная автоматизация процессов с использованием API для предоставления сервисов, управления платформами и непрерывного развертывания (continuous deployment).

Несмотря на быстрое и широкое распространение, API остаются плохо защищенными, а автоматизированные угрозы растут. Личные сведения (Personally identifiable information, PII), данные платежных карт и критически важные для бизнеса сервисы подвергаются риску из-за атак ботов.

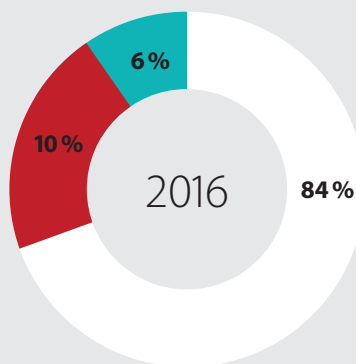
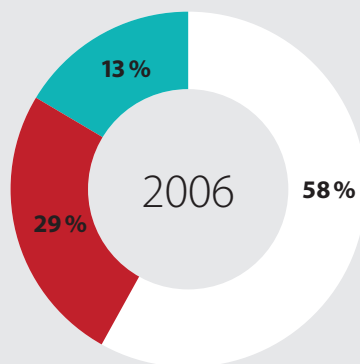


Рисунок 1. Распределение протоколов и стилей API на основе каталога API, перечисленных в источнике ProgrammableWeb

Май 2016 г.

● REST ● SOAP ● Другие

ПРИЗНАКИ АТАК БОТОВ НА API

- Одиночный HTTP-запрос (от уникального браузера, сессии или устройства)
- Увеличение частоты ошибок (например, код состояния HTTP 404, сбои проверки данных, сбои авторизации и т. д.)
- Чрезвычайно высокая интенсивность использования приложений с одного IP-адреса или токена API
- Внезапный всплеск использования API с больших распределенных IP-адресов
- Высокое соотношение запросов GET/POST к HEAD для пользователя, сессии, IP-адреса или токена API по сравнению с легитимными пользователями.

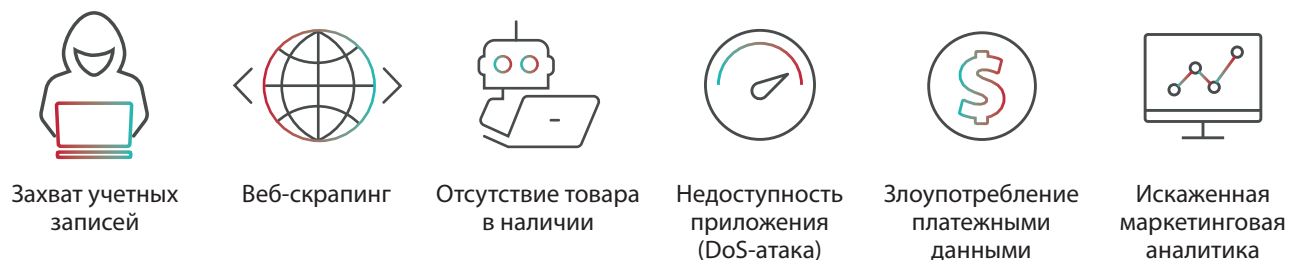


Рисунок 2. Наиболее распространенные автоматизированные угрозы, нацеленные на API

КЛЮЧЕВЫЕ УЯЗВИМОСТИ API И АВТОМАТИЗИРОВАННЫЕ АТАКИ

1. Недостатки проверки подлинности и захват учетных записей

Когда запрос поступает от разрешенного пользователя, многие API не проверяют статус аутентификации. Злоумышленники используют различные способы эксплуатации подобных недостатков, такие как перехват сессии и агрегация учетных записей для имитации разрешенных вызовов API. Злоумышленники также реконструируют (reverse engineer) мобильные приложения, чтобы узнать, как вызываются API. Если ключи API встроены в приложение, возможен взлом API. Ключи API не следует использовать для аутентификации пользователя. Киберпреступники также осуществляют атаки с использованием украденных учетных данных для захвата учетных записей пользователей. Radware Bot Manager блокирует попытки сканирования API в поисках уязвимостей и защищает критически важные для бизнеса API от автоматизированных атак. Это решение также анализирует запросы API для обнаружения и блокирования вредоносных попыток уклониться от идентификации источника и снятия цифрового отпечатка устройства, а также прямого доступа к API.

2. Отсутствие надежного шифрования

Многим API не хватает надежного шифрования между клиентом API и сервером. Злоумышленники используют уязвимости с помощью атак «злоумышленник в середине» - с вмешательством в соединение. Злоумышленники перехватывают незашифрованные или плохо защищенные API-транзакции для кражи конфиденциальной информации или изменения данных транзакций. Кроме того, повсеместное использование мобильных устройств, облачных систем и шаблонов проектирования микросервисов еще больше усложняет задачу защиты API, так как теперь для обеспечения совместимости разнородных веб-приложений задействованы многочисленные шлюзы. Шифрование данных, передаваемых по всем этим каналам, имеет первостепенное значение. Radware Bot Manager защищает API от периферии до конечных точек для обеспечения безопасного обмена данными.

Рисунок 3. 56 % API не относятся к стандартным веб- или мобильным API, им требуется индивидуальное решение безопасности

(Источник: Отчет о состоянии API на 2019, SMARTBEAR)



3. Уязвимость бизнес-логики

API уязвимы для злоупотреблений бизнес-логикой. Именно поэтому требуется специализированное решение для управления ботами, а применение эвристического анализа, который хорошо работает для мобильных и веб-приложений, может привести к множеству ошибок - ложноположительных и ложноотрицательных срабатываний. Решение Radware изучает коммуникационный поток и контекст вызовов, а также использует аутентификацию запрос-ответ (например, CAPTCHA) при подозрительных вызовах API для предотвращения потенциальных попыток злоупотребления бизнес-логикой. Ответы на эти запросы помогают Radware построить замкнутую систему обратной связи, которая динамически улучшает модели машинного обучения Bot Manager.

4. Плохая защита конечных точек

Большинство IoT-устройств и инструментов микросервисов запрограммированы на взаимодействие с сервером по API-каналам. Эти устройства аутентифицируются на серверах API с использованием клиентских сертификатов. Хакеры пытаются получить контроль над API из конечной точки IoT. Если им это удастся, они могут легко изменить порядок API, что приводит к нарушению безопасности данных. Radware использует аналитические данные, собранные на основе своей глобальной клиентской базы, для принятия превентивных мер против потенциальных попыток незаконного доступа к конечным точкам IoT и инструментам микросервисов.

КОНТРОЛЬНЫЙ СПИСОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ API

Эти девять лучших практик обязательны для защиты ваших инфраструктур API от взлома и злоупотреблений.

- Мониторинг и управление вызовами API от автоматизированных скриптов (ботов)
- Отказ от использования примитивной аутентификации
- Внедрение мер по предотвращению доступа к API со стороны изодрённых, имитирующих поведение человека ботов
- Надежное шифрование имеет решающее значение
- Ограничение частоты запросов (rate limiting) на основе токенов, оснащенное функциями ограничения доступа к API разрешенным количеством IP-адресов, сессий и токенов
- Всестороннее протоколирование запросов и ответов
- Сканирование входящих запросов на злонамеренность
- Поддержка кластерной реализации API для обеспечения отказоустойчивости
- Отслеживание использования и перемещения вызовов API для поиска аномалий

RADWARE BOT MANAGER ЗАЩИЩАЕТ API

Radware Bot Manager защищает API от автоматизированных атак, чтобы только законные пользователи и устройства могли получить доступ к API, блокируя любые попытки реконструирования (reverse engineer) мобильных SDK. В решение Radware используется проприетарный механизм глубокого анализа поведения на основе намерений (IDBA), позволяющий проанализировать намерение, стоящее за запросом API, и блокировать вредоносную активность. Это решение опирается на коллективный опыт на основе данных профилей ботов и цифровых отпечатков устройств для оптимизации точности обнаружения и интегрируется в существующую инфраструктуру без каких-либо изменений стека технологий.

КАК RADWARE BOT MANAGER РЕШАЕТ ПРОБЛЕМУ ВРЕДНОСНЫХ БОТОВ, НАЦЕЛЕННЫХ НА API

Управление потоками в API — защита межмашинного взаимодействия (Machine to Machine) и IoT	Клиентские SDK для API — защита API межмашинного взаимодействий
Каждый API — это узел, и вероятность перемещения потока от одного узла к другому представлена архитектурным весом. Потоки с низкой вероятностью блокируются.	Эффективное получение цифровых отпечатков и уникальная идентификация источников атак посредством API для обнаружения атак ботов на API с помощью нового, уникального, независимого от приложений SDK.
Контекст вызовов — защита веб- и мобильных API	Поток аутентификации — защита АТО для API
Запрет прямого доступа к API без предыдущей веб-транзакции или вызова с мобильного устройства.	Проверка законности доступа к активам. Обнаружить поток неудачного входа в систему и блокировать источник атаки, генерирующий несколько неудачных попыток входа посредством API.

ВОСЕМЬ ПРЕИМУЩЕСТВ RADWARE BOT MANAGER ДЛЯ API

1. Специализированное решение для предотвращения злоупотреблений API

Решение Radware Bot Manager для API специально разработано для учета всех автоматизированных угроз для API. В данном решении используется расширенное машинное обучение, которое напоминает среду API и структуры внутреннего взаимодействия. Решение отслеживает контекст вызовов и позволяет управлять потоком для обнаружения и предотвращения любой вредоносной активности.

2. Широкий охват и точное обнаружение атак для защиты конфиденциальной информации

Radware Bot Manager защищает API от изоциренных ботов в режиме реального времени. Он перехватывает ответ службы API и собирает необходимые данные для точного отслеживания всех случаев входа/аутентификации и предотвращения захвата учетных записей (заполнение, взлом учетных данных) для API аутентификации.

3. Защита API от периферии до конечных точек

Защита пограничных шлюзов, микрошлюзов и микросервисов для обеспечения комплексной безопасности API.

4. Накопленные сведения по ботам

Информационный архив сигнатур и цифровых отпечатков ботов на основе данных глобальной клиентской базы позволяет принимать превентивные меры против попыток проникновения со стороны вредоносных ботов. Накопленные сведения по ботам, собранные путем постоянного автоматизированного анализа огромного массива данных Интернета и даркнета, позволяют инициировать нотификации до атаки.

5. Комплексная отчетность и аналитика

Radware предлагает готовые подробные отчеты для всех семейств ботов, включая оффлайн-аналитику на основе токенов. Организации могут отслеживать автоматизированные операции на основе пользовательских агентов, географии, ссылок и целевых страниц. Доступны API визуализации для сбора данных, управления ими и создания отчетов.

6. Гибкие варианты развертывания

Radware предлагает гибкие варианты развертывания, в том числе развертывание по требованию, локальное и облачное для различных инфраструктур. Варианты интеграции включают плагины CDN, теги JavaScript, плагины веб-серверов и облачные соединители API. Другие варианты — SDK для мобильных устройств и виртуальное устройство.

7. Полный пакет для защиты приложений и API

Простая интеграция с брандмауэром веб-приложений Radware (WAF) и решениями по предотвращению DDoS-атак локально и в облаке.

8. Полностью управляемый сервис

Облачный сервис безопасности, интегрированный с облачным брандмауэром WAF компании Radware, обеспечивают эффективность интеграции, создания отчетов и настройки с использованием унифицированного портала.



ООО "ТИК" - официальный партнер Radware в России
+7 (495) 231-21-20 | info@teleincom.ru | www.teleincom.ru

О КОМПАНИИ RADWARE

Radware® (NASDAQ: RDWR) — мировой лидер в области создания решений для обеспечения **кибербезопасности** и **доставки приложений** для физических, облачных и программно-определяемых центров обработки данных. Отмеченные наградами решения компании обеспечивают цифровую безопасность предприятий по всему миру, включая защиту и доступность инфраструктуры, 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. Дополнительные сведения на сайте www.radware.com.

Компания Radware приглашает вас присоединиться к нашему сообществу и следить за новостями на наших ресурсах: [блог Radware](#), [LinkedIn](#), [Facebook](#), [Twitter](#), [SlideShare](#), [YouTube](#), приложение [Radware Connect](#) для iPhone® и наш центр безопасности DDoSWarriors.com, который обеспечивает всесторонний анализ инструментов, тенденций и угроз распределенных атак типа «отказ в обслуживании».

Документ предоставлен исключительно в информационных целях. Документ может содержать ошибки и не является объектом никаких гарантий или условий, выраженных устно либо подразумеваемых на основании закона. Компания Radware отказывается от любых обязательств по этому документу, а также заявляет, что документ не подразумевает прямо или косвенно никаких обязательств по договору. Технологии, функции, службы и процессы, описанные в документе, могут быть изменены без уведомления.

© Radware, 2020. Все права защищены. Продукты и решения компании Radware, упомянутые в данном документе, защищены товарными знаками, патентами и заявками на патенты, находящимися на рассмотрении, компании Radware в США и других странах. Дополнительная информация по адресу <https://www.radware.com/LegalNotice/>. Все другие товарные знаки и наименования являются собственностью соответствующих владельцев.