**УДК 004** **Информационные технологии**

***Голубятников Артем Олегович,*** *студент кафедры защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург*

# DDOS-АТАКИ И МЕТОДЫ БОРЬБЫ С НИМИ

**Аннотация:** данная статья посвящена DDoS-атакам, приводится определение, причины, типы DDoS-атак. В работе рассматриваются подходы и сервисы по защите.

**Ключевые слова:** DDoS, атака, защита, траффик, основные типы, сервисы, уровни обслуживания.

**Abstract:** this article is devoted to DDoS attacks, the definition, causes, types of DDoS attacks are given. The paper discusses approaches and services for protection.

**Keywords:** DDoS, attack, protection, traffic, main types, services, service levels.

## Что такое DDoS-атака?

Это способ залить сеть, ОС или приложение большим объемом трафика, подключений или запросов, чем они могут обработать. Это может иметь катастрофические последствия для бизнеса и других типов организаций, таких как правительство.

Для основных веб-сайтов и приложений даже несколько секунд простоя могут привести к значительной потере доходов и перебоям в предоставлении услуг. DDoS — это ненавязчивая атака, следовательно злоумышленнику не нужен доступ администратора к вашему сайту или приложению для его запуска, и этот трафик может сначала выглядеть как обычно [5].

DDoS атака запускается с многочисленных скомпрометированных устройств, а также из нескольких разных сетей, часто распределенных по миру в так называемой botnet. Botnet — это группа компьютеров, зараженных вредоносным программным обеспечением (вредоносным ПО). В этом основное отличие от атаки типа «отказ в обслуживании» (DoS), при которой используется одно устройство или же одна сеть.

**Почему существуют DDoS-атаки?**

DDoS-атаки могут быть запущены по разным причинам, от активности до спонсируемых государством сбоев, причем многие атаки осуществляются просто для получения прибыли. Приобрести онлайн-сервисы для DDoS-атак относительно недорого, особенно в соотношении размера ущерба, который они могут нанести.

Почему DDoS является проблемой и на что это влияет?

Доступность ваших приложений или веб-сайтов. Атаки могут длиться часами или даже днями и мешают вашим пользователям нормально использовать ваши приложения [5].

Финансовые последствия для вашего бизнеса: упущенная выгода, увеличение расходов на обеспечение ИТ-инфраструктуры.

Безопасность ваших данных: DDoS-атаки могут привести к потере данных.

Репутация ваших приложений: имя вашего бренда получает урон и теряет доверие.

**Основные типы DDoS-атак?**

DDoS-атаки можно в основном разделить по тому, какой уровень модели взаимодействия открытых систем (OSI) они атакуют.

Атаки прикладного уровня (уровень 7) — HTTP-флуд, DNS-запросы: состоят из запросов (популярны HTTP GET и DNS-запросы), предназначенных для потребления ресурсов приложения (память, ЦП, полоса пропускания) [4]. Примером может служить злоумышленник, который постоянно использует функции веб-сайта (отправляя контактную форму или любые запросы API),

когда он знает, что это вызывает обработку базы данных и приложений, так что базовая веб-служба занята вредоносными запросами и не может доставлять их другим пользователям. больше. Основная трудность при попытке смягчить атаку прикладного уровня заключается в различении обычного и вредоносного трафика [3].

Атаки с исчерпанием состояния (уровень 4) — SYN Flood: потребляют таблицы состояний TCP-соединений, присутствующие во многих сетевых инфраструктурах и устройствах безопасности, включая маршрутизаторы, брандмауэры и балансировщики нагрузки, а также сами серверы приложений [4]. Злоумышленник быстро инициирует подключение к серверу, не завершая соединение. Эти атаки могут заблокировать доступ для законных пользователей или вывести из строя устройства безопасности, иногда даже оставляя средства защиты широко открытыми для кражи данных. Этот тип DDoS-атаки использовался в атаке DYN в 2016 году, в результате веб-сайты, такие как Amazon, Twitter, Github и другие, стали недоступны.

Объемные атаки (уровень 3): также называются сетевыми флудами и включают UDP-флуд и ICMP-флуд. Этот тип атаки возникает, когда сеть перегружена большим объемом вредоносного трафика, в результате чего ваши приложения или службы становятся непригодными для пользования. Как правило, этот тип атаки описывается в сотнях Гбит/с, но некоторые из недавних атак масштабируются до более чем 1 Тбит/с.

**Подходы к противодействию DDoS-атакам в целом**

На этом этапе вы должны понимать, что не существует простого способа избежать DDoS-атаки, но есть некоторые методы защиты от таких атак:

Непрерывный мониторинг емкости (загрузка ЦП системы, нагрузка входящего трафика и т. д.), типа трафика и любой критической инфраструктуры и службы (например, брандмауэры и т. д.) [2].

Сегментация внутренних и внешних сетей и любой сети, содержащей критически важные системы.

Используйте облачный хостинг от крупного поставщика облачных услуг

с высокой пропускной способностью и CDN (сетью доставки контента), который кэширует веб-сайты или данные приложений. Если вы используете сеть доставки контента, избегайте раскрытия IP-адреса исходного веб-сервера и используйте брандмауэр, чтобы только служба CDN могла получить доступ к этому веб-серверу.

Внедрите мониторинг доступности с оповещениями в реальном времени для обнаружения DDoS-атак и измерения их воздействия.

**Более конкретные методы смягчения DDoS-атак:**

Тщательно планируйте масштаб своей инфраструктуры: большинство DDoS-атак основаны на большом объеме и пытаются исчерпать возможности ваших ресурсов [3]. Что касается пропускной способности, убедитесь, что ваш хостинг-провайдер предоставляет надежное подключение к Интернету, которое имеет возможность обрабатывать большие объемы трафика. Для серверов важно, чтобы вы могли быстро увеличить или уменьшить свои вычислительные ресурсы или чтобы у вас было достаточно ресурсов с самого начала. Также рекомендуется использовать балансировщики нагрузки для перераспределения нагрузки между серверами, чтобы предотвратить перегрузку одного из серверов.

Уменьшите площадь поверхности вашей сети: создайте минимальную «поверхность», которую можно атаковать, и создайте защиту в одном месте. Ваше приложение или ресурсы должны блокировать любую связь с любыми портами, протоколами или приложениями из неожиданных источников. Вы можете использовать брандмауэры или списки контроля доступа (ACL), чтобы контролировать, какой трафик достигает ваших приложений. Вы также можете разместить свои ресурсы за сетью доставки контента (CDN) или балансировщиком нагрузки.

**Сервисы AWS для защиты от DDoS-атак**

Во-первых, полезно увидеть несколько примеров архитектуры, которые помогут вам понять, как лучше всего смягчить и защитить ваше приложение от возможных DDoS-атак.

Эта эталонная архитектура включает в себя несколько пограничных сервисов AWS, которые могут помочь вам повысить устойчивость вашего веб-приложения к DDoS-атакам, а также защитить ваше приложение и инфраструктуру другими способами. Эта архитектура предназначена для тех, кто использует только сервисы AWS [1].

**Существует два уровня обслуживания:**

AWS Shield Standard может быть использован любым пользователем ПК без дополнительной платы [1]. Он защищает вас от 96% известных атак на 3 и 4 уровнях. Эта защита автоматически и прозрачно применяется к балансировщикам Elastic Load Balancer, дистрибутивам Amazon CloudFront и AWS Route 53.

**Преимущества AWS Shield Standard:**

Защита от DDoS-атак: AWS Shield Standard проверяет входящий трафик в вашу сеть и применяет комбинацию сигнатур трафика, алгоритмов обнаружения аномалий и других методов анализа для обнаружения вредоносного трафика. Он устанавливает некоторые статические пороговые значения для каждого из ваших типов ресурсов, но не обеспечивает никаких пользовательских средств защиты.

Видимость атак: вам предоставляется общая информация о DDoS-атаках в сети AWS. Эту информацию можно найти в Консоли управления AWS на панели управления глобальными угрозами.

**Библиографический список:**

1. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4. – С. 76-84.

2. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.

3. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 570-573.

4. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 590-595.

5. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.