99. СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ОТ DDOS-АТАК

Лис М.О., студент гр.373904, Федюкович Т.В., ассистент каф. ЭИ
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ефремов А.А. – канд. экон. наук, доцент каф. ЭИ

Аннотация: в статье рассматриваются современные методы защиты от распределённых атак типа «отказ в обслуживании» (DDoS). Проведён обзор основных техник, применяемых для минимизации воздействия таких атак на информационные системы. В статье анализируются как традиционные, так и новые подходы к обеспечению безопасности, включая облачные технологии, машинное обучение и адаптивные системы обнаружения и реагирования на атаки.

Ключевые слова: DDoS-атаки, защита от DDoS, кибербезопасность, облачные решения, машинное обучение, фильтрация трафика, гибридные системы, аппаратные брандмауэры, обнаружение аномалий, адаптивная защита.

В современном мире, где информационные технологии играют критическую роль в поддержании бизнес-процессов, государственной деятельности и общественной жизни, защита от кибератак становится все более актуальной задачей. Одной из наиболее разрушительных и распространенных форм киберугроз являются распределенные атаки типа «отказ в обслуживании» (DDoS), цель которых – нарушить работу веб-сервисов, сетевой инфраструктуры или серверов путем искусственного создания чрезмерной нагрузки.

В отличие от обычной DoS-атаки, которая исходит от одного источника, DDoS-атака включает в себя множество атакующих источников, которые могут быть распределены по всему миру. Это усложняет задачу блокирования атаки, так как трафик приходит с множества IP-адресов.

Атакующие генерируют огромное количество трафика к целевому ресурсу. Это может быть реализовано через чрезмерное массовое направление запросов серверу или через более сложные методы, такие как эксплуатация специфических уязвимостей протоколов.

Некоторые DDoS-атаки используют особенности сетевых протоколов, например, SYN Flood, где злоумышленник начинает TCP-сессию, но не завершает её, вызывая истощение ресурсов сервера.

Часто для проведения DDoS-атак используются ботнеты – сети заражённых устройств (компьютеры, смартфоны, IoT-устройства), контролируемые атакующим. Каждое устройство в ботнете может отправлять запросы или пакеты данных к цели, создавая колоссальную нагрузку [1].

На рисунке 1 представлен принцип действия DDoS-атаки.

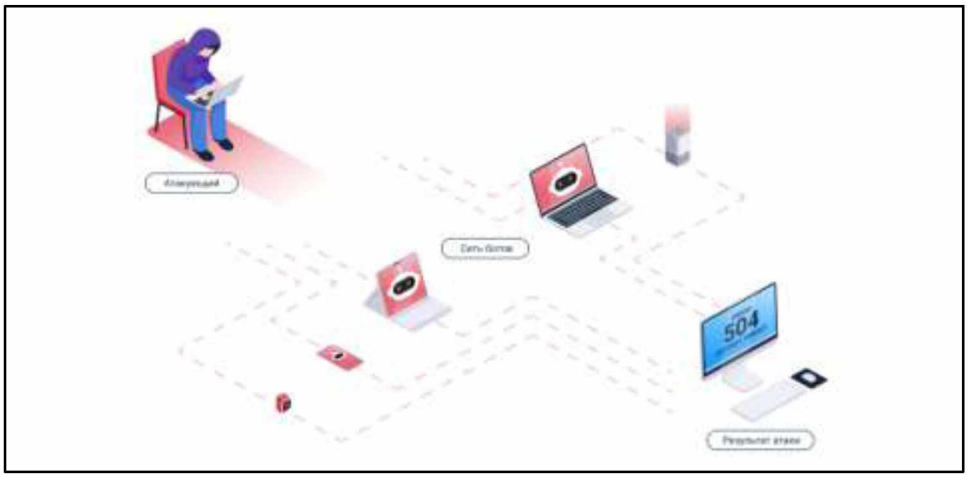

Рисунок 1 – Принцип действия DDoS-атаки [2]

Существуют следующие типы DDoS-атак:

Volumetric attacks: Направлены на исчерпание широкополосного доступа жертвы. Примером может служить UDP flood.

Protocol attacks: Эти атаки нацелены на определённые аспекты протоколов. Пример – SYN flood, когда атакующий отправляет большое количество запросов на установление соединения, не завершая их.

Application layer attacks: Атаки на прикладной уровень (например, HTTP flood), которые маскируются под законные запросы, но их цель –исчерпать ресурсы приложения или сервера.

DDoS-атаки развиваются вместе с технологиями: увеличиваются их масштабы, сложность и способность обходить традиционные методы защиты. Это обуславливает необходимость постоянного совершенствования методов обнаружения и нейтрализации таких атак. Современные методы защиты включают в себя не только улучшение существующих технологий, но и разработку новых подходов, способных предвидеть и адаптироваться к изменениям в стратегиях злоумышленников.

Рассмотрим традиционные методы защиты от DDoS-атак. Фильтрация трафика остаётся одним из наиболее распространённых подходов к защите от DDoS. Этот метод позволяет идентифицировать и отсекать потенциально вредоносный трафик на основе заранее определённых критериев, таких как IP-адреса, типы протоколов или порты. Современные фильтры способны динамически адаптироваться к меняющимся паттернам атак, что делает их эффективными даже в условиях постоянно эволюционирующих угроз.

Ограничение скорости обработки запросов (rate limiting) помогает предотвратить перегрузку ресурсов путём установления максимального количества запросов, которые могут быть обработаны в единицу времени. Этот метод особенно эффективен против атак, нацеленных на исчерпание системных ресурсов, таких как сетевая пропускная способность или процессорное время. [3]

Сетевые брандмауэры и системы предотвращения вторжений (IPS) предоставляют дополнительный уровень защиты, блокируя трафик, который соответствует известным образцам вредоносной активности. Эти системы постоянно обновляются для отражения новейших угроз и тактик атакующих, что делает их незаменимыми в борьбе с DDoS.

В современной борьбе с DDoS-атаками облачные и гибридные решения играют ключевую роль, предоставляя масштабируемую защиту и гибкость для эффективного распределения ресурсов. Эти технологии сочетают мощь облачных сервисов с надёжностью локальных систем, обеспечивая комплексный подход к защите от киберугроз.

Облачные сервисы, такие как AWS Shield, Cloudflare и Google Cloud Armor, предоставляют масштабируемую защиту, которая может адаптироваться к изменяющейся интенсивности атак. Распределение трафика по нескольким центрам обработки данных позволяет минимизировать его воздействие на любой один ресурс, тем самым затрудняя проведение успешной атаки. Также облачные провайдеры предлагают специализированные услуги, направленные на митигацию DDoS, которые включают в себя расширенные настройки фильтрации и автоматическое распределение нагрузки.

Гибридные системы сочетают локальные и облачные элементы защиты, предлагая уникальную комбинацию глубины и гибкости. Это позволяет организациям использовать сильные стороны каждого подхода, оптимизируя свою защиту и обеспечивая бесперебойную работу при максимальной нагрузке.

Методы защиты от DDoS-атак с использованием машинного обучения (ML) и искусственного интеллекта (AI) представляют собой передовые подходы, направленные на повышение эффективности и оперативности обнаружения и реагирования на киберугрозы.

Машинное обучение особенно эффективно в обнаружении аномалий в сетевом трафике, что является критическим аспектом защиты от DDoS. Системы, основанные на ML, анализируют образцы трафика и учатся распознавать отклонения от нормы, которые могут указывать на начало атаки. Преимущество таких систем заключается в их способности адаптироваться к новым угрозам без необходимости предварительного программирования специфических правил или сигнатур.

Используя алгоритмы искусственного интеллекта, системы могут не только обнаруживать текущие или начинающиеся атаки, но и прогнозировать потенциальные угрозы на основе анализа тенденций и поведения трафика. Это позволяет предпринимать весомые шаги для предотвращения атак, ещё до того, как они окажут влияние на ресурсы организации.

Искусственный интеллект в защитных системах может автоматизировать процесс принятия решений о том, как реагировать на обнаруженные атаки. AI может мгновенно анализировать большие объемы данных о трафике и принимать обоснованные решения о блокировке атакующего трафика, перенаправлении его или изменении конфигурации системы для минимизации ущерба [2].

Системы на базе машинного обучения и искусственного интеллекта обладают уникальной способностью непрерывно обучаться и адаптироваться. Они могут обновлять свои модели и алгоритмы в реальном времени, что делает их более эффективными в долгосрочной перспективе по мере того, как атакующие адаптируют свои методы и стратегии.

Координация с интернет-провайдерами и другими сторонними организациями является важной частью стратегии защиты от DDoS-атак. Этот подход позволяет использовать ресурсы и возможности этих организаций для предотвращения или смягчения воздействия атак.

Современные способы защиты от DDoS-атак требуют комплексного подхода, включающего технические, программные и организационные меры. Постоянное обновление защитных технологий, обучение персонала и координация с внешними партнерами являются ключевыми элементами успешной стратегии защиты от DDoS-атак.

Список использованных источников:

1. DDoS-атаки и методы защиты от них [Электронный ресурс] Режим доступа: https://habr.com/ru/companies/slurm/articles/674218/

2. ТОП 10 способов защиты от DDoS-атак [Электронный ресурс]. – Режим доступа: https://ddos-guard.net/ru/blog/sposoby-zashity-ot-ddos-atak

3. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance / Dhruba Kumar Bhattacharyya, Jugal Kumar Kalita / Chapman and Hall/CRC, 2016 г. – С. 146-155