УДК 004.052.3

С. М. Эфендиев[1]*

Анализ существующих атак на отказ в обслуживании и известные методы противодействия им

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: cellexc@yandex.ru

Аннотация. В статье обозначены статистика и актуальность проблемы распределенных атак на отказ в обслуживании за последние 5 лет. В исследованиях отмечается рост DDoS-атак, в частности, атак с использованием протокола HTTP. Разбираются методы и подходы злоумышленников для проведения атак на информационные системы и ресурсы типа «отказа в обслуживании» с целью последующего выведения из строя информационных систем. В работе отмечается важность исследования существующих методов и атак злоумышленников, используемых для выведения из строя современных информационных систем, с целью разработки подхода для прогнозирования новых видов атак и комплексного противодействия существующим методам злоумышленников. Отмечены существующие подходы для своевременного обнаружения атак на отказ в обслуживании и обозначены ключевые преимущества и недостатки использования таких подходов. Главные выводы подчеркивают использование комплексных и гибридных подходов и алгоритмов для обнаружения и прогнозирования атак на отказ в обслуживании и последующее противодействие таким атакам.

Ключевые слова: информационная безопасность, распределенные атаки на отказ в обслуживании, кибербезопасность, отказоустойчивость системы, DDoS атака

S. M. Efendiev[1]*

Analysis of Existing Denial of Service Attacks and Prevention Methods

[1] National Research Nuclear University «MEPhI», Moscow, Russian Federation
* e-mail: cellexc@yandex.ru

Abstract. The article outlines the statistics and relevance of problem of distributed denial of service attacks over the last 5 years. The research notes the growth of DDoS attacks, in particular, attacks using the HTTP protocol. The methods and approaches of attackers to conduct denial-of-service attacks on information systems and resources with the purpose of subsequent disabling information systems are analyzed. The paper emphasizes the importance of researching existing methods and attacks of attackers used to disable modern information systems with the purpose of developing an approach for predicting new types of attacks and complex counteraction to existing methods of attackers. Known approaches for timely detection of denial of service attacks are noted and key advantages and disadvantages of using such approaches are outlined. The main conclusions emphasize the use of integrated and hybrid approaches and algorithms for detecting and predicting denial of service attacks and subsequently countering such attacks.

Keywords: information security, distributed denial of service attacks, cyber security, system fault tolerance, DDoS attack

Введение

Развитие цифровых технологий, обработка персональных данных и критической информации в информационных системах, удобство работы с системами, недостаточная защищенность информационных активов, легкий доступ к информации позволяют злоумышленникам проводить атаки, направленные на получение конфиденциальной информации, нарушение целостности и доступности обрабатываемых данных в информационных системах. В настоящий момент самым распространённым и успешным способом реализации атак на конечные устройства (сетевые устройства, сервера, рабочие станции, IOT-устройства и др.) являются атаки на отказ в обслуживании, в частности, распределенные атаки на отказ в обслуживании.

Согласно статистике, представленной Лабораторией Касперского, количество распределенных атак на отказ в обслуживании в третьем квартале 2022 года по сравнению с третьим кварталом 2021 года выросло на 47 % [1]. Заметен значительный рост атак на прикладной уровень модели TCP/IP в виду того, что такие атаки сложнее обнаруживать, а также блокировать. Согласно исследованию Cloudflare, количество DDoS-атак в третьем квартале 2023 года выросло на 65 % по сравнению с вторым кварталом 2023 года, и в общей сложности зафиксировано 8,9 триллионов HTTP DDoS-запросов, которые системы Cloudflare смогли нейтрализовать [2].

Также, согласно исследованию Лаборатории Касперского, количество атак на протокол HTTPS в значительной степени превзошло количество атак на протокол TCP, хотя атаки на протокол TCP все еще остаются популярными у злоумышленников.

Таким образом, проблема отказоустойчивости и противодействия DDoS-атакам остается важной и актуальной задачей для проектируемых и создаваемых систем защиты информации от DDoS-атак.

Обсуждение

При проектировании и создании информационных систем архитекторы и разработчики уделяют большое внимание функциональным характеристикам и бизнес-функциям приложений и забывают про вопросы безопасности и отказоустойчивости приложений. Немаловажным фактором возникновения уязвимостей приложений, приводящих к проблемам отказоустойчивости, является ограниченность ресурсов, кадровый голод архитекторов и специалистов по информационной безопасности и недостаточное функциональное и нагрузочное тестирование приложений. В связи с этим возникают проблемы и уязвимости при создании и проектировании информационных систем и приложений. Например, недостатками, которые могут приводить к отказам в обслуживании, являются неэффективное масштабирование приложения и баз данных, некорректное управление ресурсами (процессор, оперативная память) и состоянием приложения, неправильная интеграция сторонних сервисов, известные уязвимости в библиотеках и используемых компонентах и др. Подобные проблемы приводят к тому,

что злоумышленник может вызвать отказ в обслуживании информационной системы или приложения за короткое время и с применением небольшого количества зараженных ресурсов (ботнет сеть).

Атаки на прикладной уровень TCP\IP можно разделить на следующие категории:

– атаки, направленные на архитектурные особенности протоколов. Примерами могут служить такие атаки, как SNMP GETBULK, NTP mode 6, DNS Amplification, HTTP/2. Приведенные атаки используют архитектурные недостатки известных протоколов, позволяющих осуществить отказ в обслуживании конечного ресурса;

– атаки, направленные на эксплуатацию известных уязвимостей, приводящих к DoS. К таким уязвимостям можно отнести уязвимости протокола SMB CVE-2017-0143 (MS-17-010), уязвимость удаленных рабочих столов CVE-2019-1181 (BlueKeep), уязвимость отказа в обслуживании программного продукта Cisco AnyConnect CVE-2023-20241, и др. [3];

– атаки большого объема. Примером таких атак может служить атака RUDY, позволяющая вызвать отказ в обслуживании приложения с использованием запросов, содержащих большой объем информации;

– медленные атаки. К медленным атакам можно отнести атаку Slowloris и атаку RUDY, которые позволяет злоумышленнику вызвать отказ в обслуживании серверных ресурсов за счет увеличения длительности соединения.

Для получения полной картины используемого злоумышленниками арсенала и методов для выполнения атак на отказ в обслуживании необходимо рассмотреть наиболее популярные атаки детально.

Атака HTTP GET DDoS. Суть атаки заключается в том, что злоумышленник выполняет специально подготовленные HTTP GET-запросы с последующей целью исчерпания ресурсов целевого сервера, используя ботнет-сеть и специально-предустановленные программы на зараженных ресурсах, с постоянным или изменяемым интервалом времени [4]. Большое количество HTTP GET запросов приводит к исчерпанию ресурсов веб-сервера. В частности, злоумышленники могут достигать успеха, постоянно изменяя заголовок User-Agent, а также другие заголовки HTTP-протокола с целью уклонения от обнаружения и последующего блокирования таких атак. Как правило, злоумышленники используют запросы к статическим страницам и применяют техники медленного чтения данных, что кратно увеличивает потребление оперативной памяти на целевом ресурсе и увеличивает время ответа веб-приложения для легитимных пользователей. Сложность фильтрации таких запросов возникает в виду блокирования доступа к целевому ресурсу для легитимных пользователей в случае некорректной и неправильной стратегии обнаружения и противодействия этому виду DDoS-атаки.

Атака HTTP POST DDoS. Суть атаки заключается в том, что злоумышленник выполняет специально подготовленные HTTP POST-запросы с последующей целью исчерпания ресурсов целевого сервера, используя ботнет-сеть и специально-предустановленные программы на зараженных ресурсах, с постоянным

или изменяемым интервалом времени [5]. Целевой сервер, получая большое количество одновременно приходящих запросов, может выйти из строя и перестать обрабатывать легитимные запросы пользователей. В отличие от HTTP GET запросов, которые могут быть кэшированы, POST запросы требуют обработки на сервере и в связи с этим могут создавать большую нагрузку на сервер. Сервер начинает обрабатывать каждый входящий HTTP запрос, что увеличивает нагрузку на CPU, оперативную память и сетевую инфраструктуру. Злоумышленники выбирают отдельные страницы и ресурсы приложений, которые могут быть подвержены отказам в обслуживании, например, множественные запросы в базу данных, взаимодействие с файловой системой, выполнение запросов к другим интегрированным серверам и системам. Сложность обнаружения и блокирования таких запросов возникает в виду того, что подобные POST запросы могут исходить от легитимных пользователей и некорректная блокировка может вызвать отказ в обслуживании системы для легитимных пользователей.

Атака Slowloris. Атака Slowloris позволяет злоумышленнику исчерпать количество одновременных соединений путем использования долгих и медленных соединений с веб-сервером [6]. Злоумышленник инициирует атаку, устанавливая множество соединений с веб-сервером, но не завершая их полностью и удерживая соединения открытыми. Злоумышленник создает множество подобных соединений с большого количества ресурсов. Постепенное увеличение медленных соединений истощает ресурсы сервера, такие как память, процессор и сетевые подключения. В результате продолжительной атаки злоумышленник имеет возможность вызвать отказ в обслуживании конечного ресурса для легитимных пользователей. Атака Slowloris приводит к истощению серверных ресурсов, уменьшая доступные потоки, память и процессорное время, а также приводит к исчерпанию количества одновременных соединений.

Атака SNMP GETBULK DDoS. Протокол SNMP работает на прикладном уровне TCP\IP и используется для обмена сообщениями между управляющей станцией и сетевыми устройствами с целью мониторинга и управления их состоянием [7]. Используя особенности протокола, злоумышленник имеет возможность отправлять большое количество GETBULK SNMP запросов к целевым устройствам. Целевое устройство выдает в 50 раз больше информации в ответ на входящий запрос, тем самым вызывая большой поток трафика, что может повлиять на различные компоненты сетевой инфраструктуры сети, такие как маршрутизаторы, коммутаторы и другие устройства, использующие протокол SNMP для мониторинга и управления. Выполняя большое количество одновременных запросов GETBULK SNMP с зараженных ресурсов, злоумышленник может вывести из строя целевое устройство.

Атака NTP mode 6. Протокол NTP используется для синхронизации времени между компьютерами и другими устройствами в сети и работает на прикладном уровне модели ISO\OSI. Используя архитектурные особенности протокола NTP, злоумышленник имеет возможность отправить запросы NTP mode 6 к целевым ресурсам, которые в ответ генерируют большой объем данных [8]. В случае, если злоумышленник использует большое количество зараженных рабо-

чих станций, целевой ресурс генерирует значительное количество трафика, что может вывести из строя целевой ресурс и сетевые устройства, а также стать недоступным для обработки и обслуживания легитимных запросов пользователей.

Атака SSL Renegotiation. Протокол SSL служит для установления и согласования между клиентом и сервером безопасного соединения для последующей передачи данных [9]. Злоумышленник, используя большое количество ресурсов, имеет возможность установить соединения с целевым ресурсом с использованием защищенного соединения и в постоянном режиме запрашивать функцию повторного подтверждения SSL – SSL Renegotiation. Повторное подтверждение соединения позволяет серверу создавать новый секретный ключ поверх уже доступного SSL-соединения. Однако, генерация нового секретного ключа требует в несколько раз больше серверных ресурсов, чем клиентских. Большое количество запросов на повторное подтверждение соединения истощает ресурсы сервера и может вызвать отказ в обслуживании сервера.

Атака Rudy. Основная суть атаки Rudy заключается в перегрузке сервера за счет использования специально сформированных HTTP POST запросов с большого количества ресурсов. Злоумышленник начинает выполнять атаку, отправляя HTTP POST запросы к веб-серверу. POST-запросы содержат большие объемы данных (например, длинные случайные последовательности строк), что может привести к замедлению обработки данных на сервере [10, 11]. Основная суть атаки заключается в том, что отправляемые данные делятся на маленькие пакеты и доставляются до конечного ресурса. Продолжительная отправка HTTP POST-запросов с большими объемами данных в небольших пакетах приводит к увеличению нагрузки на сервер и последующему отказу в обслуживании, поскольку сервер тратит больше времени на обработку каждого вредоносного HTTP POST запроса и время реакции на легитимный трафик увеличивается. Атака RUDY нацелена на веб-сервер и другие компоненты сетевой инфраструктуры, создавая состояние отказа в обслуживании и препятствуя нормальному функционированию веб-сервера.

Для обнаружения, прогнозирования и блокирования вышеприведенных атак используются различные подходы. Основными критериями при выборе алгоритмов и подходов к построению стратегии обнаружения, прогнозирования и блокирования DDoS-атак являются скорость обнаружения атак и время реакции, количество ложноположительных и ложноотрицательных срабатываний системы, сложность реализации и дороговизна внедрения, способность выявления новых (ранее неизвестных) DDoS-атак, адаптация под изменяющуюся архитектуру корпоративной сети и приложений. Для решения задач анализа и управления трафиком, а также выявления потенциально-опасного трафика проведено множество исследований и разработаны соответствующие подходы [12, 13, 14, 15]. Известные подходы для обнаружения и противодействия DDoS-атакам можно разделить на следующие категории:

– сигнатурный анализ трафика. Данный подход предполагает анализ проходящего трафика через сенсор и последующую проверку этого трафика на наличие сигнатур атаки;

– анализ трафика на наличие аномалий. Проходящий через сенсор трафик анализируется на наличие отклонений или аномалий с последующей блокировкой трафика;

– смешанный подход. Используется связь сигнатурного анализа и анализа трафика на наличие аномалий для своевременного и быстрого блокирования DDoS-трафика.

Сигнатурный анализ трафика. Данный подход используется для определения атак по конкретным сигнатурам. Такой подход может применяться как к транспортным и сетевым протоколам, так и к прикладным протоколам. Трафик в режиме онлайн подвергается сбору и последующему анализу на наличие совпадений. Например, изучаются такие свойства как IP-адрес, размер пакета, количество пакетов в секунду, обращение к конкретному URL и др. В случае наличия совпадений вредоносной сигнатуры в трафике и ранее осуществляемых атак трафик от такого IP-адреса блокируется или применяются альтернативные методы защиты. Данный подход может использовать как проверку шаблонов с использованием регулярных выражений, так и анализ трафика с использованием заранее сформированных правил. Главными преимуществами применения такого подхода при анализе трафика является скорость сравнения трафика с известными сигнатурами атак и быстрое принятие решение, а также минимальные задержки при обработке трафика и минимальное количество ложноотрицательных срабатываний. Основными недостатками такого подхода являются невозможность детектировать ранее неизвестные атаки и хранение (обработка) большого объема существующих сигнатур. Также злоумышленник имеет возможность применять методы и подход для уклонения от обнаружения, например, с использованием изменения или мутации запросов к информационным системам.

Анализ трафика на наличие аномалий. Подходы и методы, основанные на анализе аномалий трафика, кардинально отличаются от подходов сигнатурного анализа. Отличие заключается в использовании алгоритмов, которые создают портрет «идеального» пользователя или состояния системы и выявляют отклонения от нормального поведения. Подход к обнаружению DDoS-атак на основе аномалий или отклонений использует следующие алгоритмы.

Машинное обучение, такие алгоритмы как методы опорных векторов (SVM), дерево принятия решений, нейронные сети (LSTM, CNN, RNN и др.), позволяют системам эффективно использовать предварительное обучение на исторических данных трафика для обнаружения отклонений или аномального трафика и также строить защиту от DDoS-атак. Например, с использованием машинного обучения можно определить и сформировать портрет пользователя и выявлять отклонения в запросах, тем самым определяя DDoS-атаку. Основным недостатком применения таких алгоритмов является использование больших объемов данных для предварительного обучения.

Статистический анализ трафика, такие алгоритмы как анализ плотности распределения, методы временных рядов и др., анализируют трафик на основании определенных критериев во временном отрезке и при нахождении отклонений или

аномалий (сезонные всплески, неожиданное увеличение плотности трафика и др.) могут принимать решение о последующей блокировке трафика. Главными преимуществами использования таких алгоритмов являются простота, так как они не требуют больших вычислительных ресурсов, и адаптация к изменяющейся архитектуре сетей. Недостатками могут быть количество ложноположительных срабатываний, так как в сетях с высокой нагрузкой и большим количеством трафика от пользователей система не сможет учитывать контекст пользователя и нюансы сетевого поведения. Как правило, такие методы могут использоваться для быстрого обнаружения стандартных отклонений и аномалий в трафике.

Кластерный анализ позволяет без предварительного обучения системы распределять трафик по группам исходя из заданных свойств (частота запросов, IP-адреса, временной интервал, количество запросов, размеры пакетов, и др.) и определять аномалии трафика на основании заданных критериев. Основным недостатком могут быть высокие требования к вычислительным ресурсам и длительное время для обучения моделей, при этом преимуществами использования алгоритмов кластерного анализа являются высокая эффективность и скорость обнаружения атак.

Смешанный подход. Большинство современных систем используют либо сигнатурный анализ выявления DDoS-атак, либо обнаружение DDoS-атак на основе аномалий. Первый метод не сможет обнаружить новые (ранее неизвестные) DDoS-атаки, а второй метод может генерировать большое количество ложноположительных или ложноотрицательных событий. Применение нескольких связанных между собой подходов может успешно защищать информационную инфраструктуру как от известных атак, так и от DDoS-атак нулевого дня.

Заключение

В данной работе была изучена статистика распределенных атак на отказ в обслуживании и подчеркнута важность разработки комплексного подхода для обнаружения, прогнозирования и предотвращения таких атак. Были определены методы, подходы и известные типы атак злоумышленников для выведения из строя информационных систем. Обозначены известные методы и подходы для обнаружения и противодействия атакам на отказ в обслуживании. Сделан вывод о необходимости использования комплексного подхода обнаружения и предотвращения распределенных атак на отказ в обслуживании для своевременного обнаружения с высокой эффективностью и скоростью реакции. В качестве потенциального подхода для последующего исследования выбран смешанный подход для обнаружения атак на отказ в обслуживании, включающий в себя сигнатурный анализ трафика и алгоритмы машинного обучения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. DDoS-атаки в первом квартале 2022. – URL: https://securelist.ru/ddos-attacks-in-q1-2022/105045/ (Дата обращения: 15.01.2023).

2. Статистика DDoS-атак в 1 квартале 2023. – URL: https://blog.cloudflare.com/ddos-threat-report-2023-q1 (Дата обращения: 04.11.2023).

3. Описание уязвимости Cisco VPN DoS CVE-2023-20241. – URL: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8 (Дата обращения: 01.04.2023).

4. Описание работы HTTP GET Flood DDoS атаки. – URL: https://kb.mazebolt.com/knowledgebase/http-get-flood/ (Дата обращения: 01.04.2023).

5. Описание работы HTTP POST Flood DDoS атаки. – URL: https://kb.mazebolt.com/knowledgebase/http-post-flood/ (Дата обращения: 01.04.2023).

6. Описание работы Slowloris DDoS атаки. – URL: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/ (Дата обращения: 01.04.2023).

7. Описание работы SNMP GetBulk DDoS атаки. – URL: https://www.nothink.org/misc/snmp_reflected.php / (Дата обращения: 01.04.2023).

8. Описание работы NTP DoS атаки. – URL: https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/ (Дата обращения: 01.04.2023).

9. Описание работы SSL Renegotiation DDoS атаки. – URL: https://kb.mazebolt.com/knowledgebase/ssl-negotiation-flood/ (Дата обращения: 01.04.2023).

10. Описание работы RUDY DDoS атаки. – URL: https://infosecportal.ru/soft/r-u-d-y/ (Дата обращения: 01.04.2023).

11. DDoS-атаки для «самых маленьких». – URL: https://habr.com/ru/articles/701482/ (дата обращения 8.01.2023).

12. Басыня Е. А. Самоорганизующаяся система управления трафиком вычислительной сети / Е. А. Басыня, Г. А. Французова, А. В. Гунько // Доклады ТУСУР. – 2014. – № 1(31). – С. 179–184.

13. Басыня Е. А. Разработка модуля системы обнаружения вторжений / Басыня Е.А. Равтович Ю.К. // Современные материалы, техника и технологии – 2016 - № 2(5) – С. 27-32.

14. Басыня, Е. А. Система интеллектуально-адаптивного управления информационной инфраструктурой предприятия / Е. А. Басыня // Информационные технологии. – 2020. – Т. 26, № 5. – С. 283-289. – DOI 10.17587/it.26.283-289.

15. Ahmad Z, Khan AS, Shiang CW, Abdullah J, Ahmad F (2021) Network intrusion detection system: a systematic study of machine learning and deep learning approaches. Trans Emerg Telecommun Technol 32:e4150.