МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛЬ-ХОРАЗМИЙ

На правах рукописи

УДК 004.492.4

МЕДЕТОВА КУНДУЗ МУРАТОВНА

«Разработка методики защиты от атак типа DDoS»

5А330601 – Программный инжиниринг

Диссертационная работа для получения академической степени магистра

Диссертация была рассмотрена и рекомендуется для защиты
Заведующий кафедрой “Программное обеспечение информационных технологий”, д.т.н.

_____О.Ж. Бабомурадов

«___»_____2018 год

Научный руководитель:
Заведующий кафедрой “Системное и прикладное программирование”
Кандидат технических наук, доцент

_____ К.Ф. Керимов

«___»_____2018 год

ТАШКЕНТ 2018

МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛЬ-ХОРАЗМИ

Факультет: Программный инжиниринг
Кафедра: Программное обеспечение информационных технологий
Учебный год: 2017-2018 гг.

Студент магистратуры: Медетова К.М.
Научный руководитель: Керимов К.Ф.
Специальность: 5А330601- Программный инжиниринг

АННОТАЦИЯ МАГИСТЕРСКОЙ ДИССЕРТАЦИИ

Актуальность работы. Одной из основных тенденций последних лет в сфере компьютерных преступлений является рост количества и сложности атак на доступность информации (ресурсов автоматизированной системы), как один из трех основных критериев (наряду с конфиденциальностью и целостностью) информационной безопасности объекта. Данные атаки образуют класс атак типа «отказ в обслуживании» (DoS - атаки). В этот класс попадают атаки на компьютерную систему, цель которых - довести систему до такого состояния, в котором её легитимные пользователи не смогут получить доступ к предоставляемым системой ресурсам (серверам, сервисам), либо этот доступ будет затруднён. Если атака выполняется одновременно с большого числа компьютеров, имеет место DDoS – атака (Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). Таким образом, разработка системы обнаружения и защиты от распределенных атак типа «отказ в обслуживании» является актуальной и практически важной задачей.

Цель работы. Цель диссертационной работы заключается в разработке и практической реализации методики защиты от распределенных атак типа «отказ в обслуживании» в компьютерных сетях.

Задачи исследования. Для достижения поставленной цели были определены и решены следующие задачи:

1. Анализ проблемы обнаружения распределенных атак типа «отказ в обслуживании» и классификация существующих DDoS - атак, методов и средств их обнаружения.

2. Построение математической модели атак типа «отказ в обслуживании» в сетях массового обслуживания и метода их обнаружения.

3. Разработка архитектуры и реализация программно-аналитического комплекса для имитационного моделирования и расчета статистических характеристик сетей массового обслуживания.

4. Разработка архитектуры и реализация программно-аналитического комплекса, предназначенного для обнаружения низкоактивных атак типа «отказ в обслуживании» в распределенных компьютерных сетях на основе разработанной методики.

Методы исследования. В диссертационной работ используются методы математического моделирования, и математической статистики сетей массового обслуживания. Полученные теоретические результаты подтверждены экспериментальными исследованиями, выполненными с применением среды программирования Microsoft Visual C++ и библиотек OpenMP, Boost, WinPcap.

Практическая значимость исследования. Разработанные модели могут быть обобщены для целей решения достаточно большого класса задач, в частности, задачи информационной борьбы в Интернет, конкуренции в сфере электронного бизнеса и др. Элементы разработанных моделей, в частности предложенные классификации механизмов защиты от атак DDoS, можно использовать для анализа систем защиты такого рода.

Объектами исследования являются распределенные компьютерные сети, процессы передачи информации и конкретные реализации атак типа «отказ в обслуживании» на ресурсы информационной системы.

Предметами исследования выступают модели и методы моделирования вычислительных сетей сетями массового обслуживания, а также методы обнаружения распределенных атак типа «отказ в обслуживании».

Структура и объем работы. Диссертация состоит из 3-х глав, выводов, ссылок и приложений.

Научный руководитель: _____ Керимов К.Ф.

Студент магистратуры: _____ Медетова К.М.

THE MINISTRY FOR DEVELOPMENT OF INFORMATION TECHNOLOGIES AND COMMUNICATIONS OF THE REPUBLIC OF UZBEKISTAN

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES NAMED MUHAMMAD AL-KHWARIZMI

Faculty: Computer Engineering

Department: Computer Systems

Academic year:2017-2018 yy.

Undergraduate: Medetova K.M.

Research supervisor: Kerimov K.F.

Specialty: 5A330601«Software Engineering

THE SUMMARY TO THE MASTER THESIS

Relevance of the research. Today there is a rapid development of network threats to computing services. At the same time, these systems are very complex, so with their development, hackers have more and more opportunities to conduct successful attacks on Web sites. This master's thesis describes the universal architecture of the system for protecting computing environments from DDoS-attacks, which includes components for automatic detection of DDoS-attacks. The models for detecting an attack on the network are based on the rules of traffic management and the extraction of malicious requests. The dissertation presents the results of experiments using various types of DDoS-attacks.

The purpose of the study. The purpose of the thesis is to develop and implement the method of protection against distributed denial of service attacks in computer networks.

Research Objectives. To achieve this goal, the following tasks were identified and solved:

1. Analysis of the problem of detection of distributed denial of service attacks and classification of existing DDoS attacks, methods and means of their detection.
2. Construction of a mathematical model of denial-of-service attacks in queuing networks and the method for detecting them.
3. Development of the architecture and implementation of the software and analysis complex for simulation and calculation of statistical characteristics of queuing networks.

4. Development of the architecture and implementation of a software analytical complex designed to detect low-activity denial-of-service attacks in distributed computer networks based on the developed methodology.

Research methods. In the dissertation, methods of mathematical modeling, and mathematical statistics of queuing networks are used. The obtained theoretical results are confirmed by experimental studies performed using Microsoft Visual C ++ programming environment and OpenMP, Boost, WinPcap libraries.

The importance of practical research work. The developed models can be generalized for the purpose of solving a fairly large class of problems, in particular, the tasks of information struggle in the Internet, competition in the field of electronic business, etc. Elements of the developed models, in particular, the proposed classifications of defense mechanisms against DDoS attacks, can be used for the analysis of defense systems of such kind.

Objects of the research. The objects of the research are distributed computer networks, information transfer processes and specific implementations of denial of service attacks on information system resources.

The subjects of the research. The subjects of the research are models and methods for modeling computer networks by queuing networks, as well as methods for detecting distributed denial-of-service attacks.

Structure and scope of work. Dissertation work consists of 3 chapters, conclusion, references and attachments.

Research supervisor _____ Kerimov K.F.

Undergraduate _____ Medetova K.M.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Развитие информационно-коммуникационных технологий (ИКТ), являющееся важнейшим фактором поднятия благосостояния и экономического роста, становится одним из основных приоритетов государственной политики Узбекистана.

Инициатива Первого Президента Республики Узбекистан послужила сигналом к крупным стратегическим изменениям. Правительство сейчас четко осознает важность ИКТ для достижения своих целей развития. Поэтому, в последние годы руководство республики принимает энергичные меры по развитию и широкому внедрению ИКТ в различные сферы общественного и государственного строительства. [1]

Общемировые процессы информационной глобализации диктуют не только необходимость повсеместного внедрения ИКТ в экономике и сферах жизни стран, но и условия обеспечения безопасности информационных систем. Узбекистан одним из первых в Центральной Азии присоединился к международной системе безопасности в сфере информационных и коммуникационных технологий.

Министерством по развитию информационных технологий и коммуникаций Узбекистана совместно с другими заинтересованными министерствами и ведомствами страны ведется разработка концепции информационной безопасности Республики Узбекистан, в которой будут определены стратегические задачи и концептуальные направления в сфере противодействия киберугрозам. [2]

DDoS-атака – распределенная атака, направленная на отказ в обслуживании. В результате атаки такого типа атакуемый сетевой ресурс получает лавинообразное количество запросов, которые не успевает обработать. Источником вредоносных запросов являются так называемые зомби-сети, состоящие большей частью из компьютеров обычных пользователей, в силу

каких-то причин зараженных вредоносным ПО. Крупным DDoS-атакам подвергаются сайты правительства и органов власти, сайты ведущих IT-корпорация Amazon, Yahoo, Microsoft и т.д. Эти мощные корпорации, имеющие огромные ресурсы, не всегда могут справиться атаками и отразить нападение.[3]

Ежегодно различные компании, предоставляющие услуги в области обеспечения информационной безопасности и противодействия кибератакам, фиксируют увеличение количества DDoS-атак и их мощность. Периодические сообщения в средствах массовой информации о недоступности тех или иных ресурсов в результате распределенных атак, направленных на отказ в обслуживании, говорят о неэффективности средств противодействия такого рода атакам. На фоне указанных выше атак к ведущим IT-корпорациям также увеличивается количество атак и к небольшим, «средним» сайтам, которые до недавнего времени не представляли интереса для злоумышленников. Однако, в настоящее время, в связи с увеличением их важности и востребованности, перебои в их работе могут быть критичными. Вместе с этим меняются и мотивы, которые движут злоумышленниками, если раньше среди причин возникновения DDoS-атак можно было выделить протест, хулиганство и т.д., то сегодня все чаще DDoS-атаки являются следствием шантажа и способом вымогательства денег. Это переводит DDoS-атаки из плоскости единичных протестных акций в область криминального бизнеса, который не ограничивается вымогательством, но и является инструментом экстремистских и террористических организаций [4]. Сегодня во всем мире стали обычной ситуацией атаки на сайты государственной власти накануне выборов или важных политических событий. Средства противодействия, специализированные именно на обеспечение безопасности небольших и средних ресурсов, получили меньшее развитие из-за преобладания в прошлом именно крупных атак. И в настоящее время отстают от эволюции самих DDoS-атак [5].

Актуальность работы. Одной из основных тенденций последних лет в сфере компьютерных преступлений является рост количества и сложности атак на доступность информации (ресурсов автоматизированной системы), как один из трех основных критериев (наряду с конфиденциальностью и целостностью) информационной безопасности объекта. Данные атаки образуют класс атак типа «отказ в обслуживании» (DoS - атаки). В этот класс попадают атаки на компьютерную систему, цель которых - довести систему до такого состояния, в котором её легитимные пользователи не смогут получить доступ к предоставляемым системой ресурсам (серверам, сервисам), либо этот доступ будет затруднён. Если атака выполняется одновременно с большого числа компьютеров, имеет место DDoS – атака (Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). За последние несколько лет количество таких атак выросло многократно и на сегодня данный класс атак имеет максимальную долю от общего числа атак. Так, в 2010 году была зафиксирована DDoS – атака с мощностью потока более 100 Гбит/сек., которая является самой мощной атакой за все время наблюдений. А в 2011 году был поставлен абсолютный рекорд по суммарному объему DDoS - трафика, который превысил трафик за все вместе взятые года предыдущих исследований. В целях минимизации последствий DDoS-атак, их обнаружение и классификация является крайне важной и вместе с тем сложной задачей. Данная проблема широко рассматривается в работах П.Д. Зегжды, Б.Н. Онукия, А.А. Молдовяна, А.В. Лукацкого, И. Яблонко, K.J. Houle, C. Patrikakis и других исследователей. Основной способ распознавания DDoS-атаки заключается в обнаружении аномалий в структуре трафика. Традиционные механизмы обеспечения безопасности - межсетевые экраны и системы обнаружения вторжений – не являются эффективными средствами для обнаружения DDoS - атак и защиты от них, особенно атак трафиком большого объема. Фундаментальной предпосылкой

для обнаружения атак является построение контрольных характеристик трафика при работе сети в штатных условиях с последующим поиском аномалий в структуре трафика (отклонения от контрольных характеристик). Аномалия сетевого трафика – это событие или условие в сети, характеризуемое статистическим отклонением от стандартной структуры трафика, полученной на основе ранее собранных профилей и контрольных характеристик. Любое отличие в структуре трафика, превышающее определенное пороговое значение, вызывает срабатывание сигнала тревоги. Вместе с тем, существующие методы обнаружения DDoS - атак, позволяющие эффективно распознавать DDoS -атаки транспортного уровня (SYN флуд, UDP-флуд и другие), мало эффективны для обнаружения низкоактивных DDoS-атак прикладного уровня («медленный» HTTP GET флуд и «медленный» HTTP POST флуд). Подробное описание этой проблемы приводится в работе W.O. Chee и T. Brennan[10]. Указанный класс DDoS-атак возник сравнительно недавно и на сегодняшний день представляет основную угрозу доступности информации в распределенных компьютерных сетях. Данные атаки приводят к потерям запросов и ответов, т.е. фактическому отказу веб-серверов на основе Microsoft IIS, Apache и других систем. Кроме того, атака может быть адаптирована для воздействия на SMTP и даже DNS-серверы. Таким образом, разработка системы обнаружения и защиты от распределенных атак типа «отказ в обслуживании» является актуальной и практически важной задачей.

Цель работы. Цель диссертационной работы заключается в разработке и практической реализации методики защиты от распределенных атак типа «отказ в обслуживании» в компьютерных сетях.

Задачи исследования для достижения поставленной цели были определены и решены следующие задачи:

1. Анализ проблемы обнаружения распределенных атак типа «отказ в обслуживании» и классификация существующих DDoS - атак, методов и средств их обнаружения.

2. Построение математической модели атак типа «отказ в обслуживании» в сетях массового обслуживания и метода их обнаружения.

3. Разработка архитектуры и реализация программно-аналитического комплекса для имитационного моделирования и расчета статистических характеристик сетей массового обслуживания.

4. Разработка архитектуры и реализация программно-аналитического комплекса, предназначенного для обнаружения низкоактивных атак типа «отказ в обслуживании» в распределенных компьютерных сетях на основе разработанной методики.

Объектами исследования являются распределенные компьютерные сети, процессы передачи информации и конкретные реализации атак типа «отказ в обслуживании» на ресурсы информационной системы.

Предметами исследования выступают модели и методы моделирования вычислительных сетей сетями массового обслуживания, а также методы обнаружения распределенных атак типа «отказ в обслуживании».

Методы исследований. В диссертационной работ используются методы математического моделирования, и математической статистики сетей массового обслуживания. Полученные теоретические результаты подтверждены экспериментальными исследованиями, выполненными с применением среды программирования Microsoft Visual C++ и библиотек OpenMP, Boost, WinPcap.

ГЛАВА 1. АНАЛИЗ СОВРЕМЕННЫХ DDOS АТАК И МЕТОДОВ ИХ ВЫЯВЛЕНИЯ

1.1 Основные понятия

Веб-сайты и сервисы (далее веб-сайт или сайт) располагаются на отдельных компьютерах, так же именуемых серверами. На этих серверах им выделяется определенная часть ресурсов для функционирования (дисковое пространство, оперативная память, процессорное время). Каждое открытие пользователем веб-страницы в браузере означает для веб-сайта то, что ему нужно занять определенную часть этих ресурсов для формирования этой страницы. Поэтому, за определенный период времени, сайт может сформировать только ограниченное число страниц. Это означает, что если сайт открыло больше пользователей, чем-то количество, на которое веб-сайт рассчитан, то часть пользователей в ответ получат либо ошибку о невозможности открыть сайт (например, сайт не доступен), либо предупреждение о перегрузке сайта с просьбой подождать (например, сайт временно недоступен, можно попробовать открыть его минут через 5-10).

Суть атаки Отказ в обслуживании (DoS) заключается в ее названии, а именно в том, что атака приводит к недоступности сайта для пользователей. Технически, это достигается за счет того, что злоумышленник постоянно открывает большое число веб-страниц, чем занимает практически все ресурсы у сайта и не дает возможность другим пользователям получить доступ к сайту. На сегодняшний день, данный вид атаки редко встречается, так как найти и определить злоумышленника очень просто - это тот, от кого постоянно идет большое число запросов на открытие страниц.

В большинстве случаев DoS атака - это мера коммерческого давления на сайты. Целью DoS атаки могут также стать политические, религиозные или иные мотивы, когда атакующие не согласны с контентом и политикой сайта.

DoS атака на сайт может быть и началом к взлому сайта, если при сбое ПО сервера или код сайта выдаёт какую-либо критическую информацию — например, версию ПО, часть программного кода, серверные пути и т. п.).

В случае, когда атака выполняется одновременно с большого числа компьютеров, говорят о DDoS-атаке (от англ. Distributed Denial of Service).

DDoS – это сокращение английского выражения Distributed Denial of Service, что переводится на русский язык как «Распределённый отказ от обслуживания». Это означает отказ от обслуживания сетевого ресурса в результате многочисленных распределенных (то есть происходящих с разных точек интернет-доступа) запросов. Отличие DoS-атаки (Denial of Service — «Отказ от обслуживания») от DDoS состоит в том, что в этом случае перегрузка происходит в результате запросов с какого-либо определенного интернет-узла.

В случае гораздо более сложной и совершенной DDoS-атаки может быть полностью нарушена работа любого ресурса — от небольшого информационного сайта до крупного интернет-магазина или почтового сервера. Во время атаки на сервер сайта - «жертвы» поступают миллионы запросов от пользователей, что приводит к его перегрузке и, соответственно, недоступности. Не успевая обрабатывать огромное количество запросов, сервер вначале начинает просто замедлять свою работу, а затем и вовсе прекращает работу. Запросы чаще всего носят хитроумный и бессмысленный характер, что еще более усложняет работу сервера.

Основная сложность для владельцев сайтов состоит в том, что огромная часть методов борьбы с DDos — практически неэффективны, ведь запросы поступают с различных сторон, и перекрыть какой-либо узел, с которого поступают запросы (как в случае в Dos-атаками) — недостаточно. Обычно атака проводится при помощи вирусных троянских программ, вовлекающих в этот процесс миллионы пользователей без их на то согласия и уведомления. Трояны

заражают недостаточно защищенные компьютеры и могут довольно долгое время действовать, вообще никак себя не обнаруживая. Зона охвата таким образом становится невероятно широкой, а запросы могут идти с самых разных сторон света.

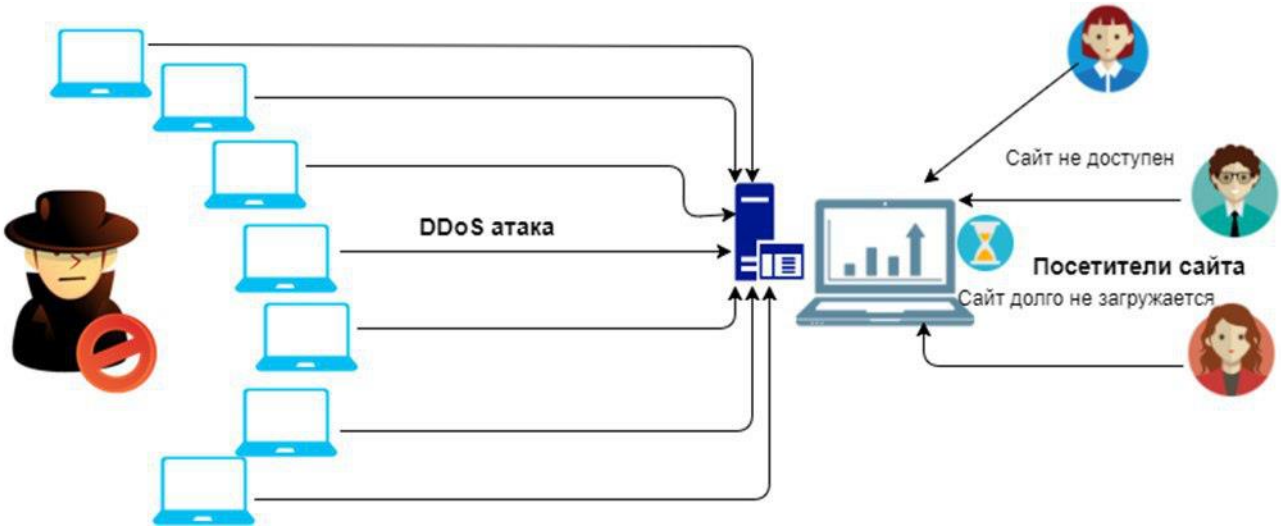

Рис.1 Схема работы DDoS атак

Зараженные компьютеры нередко называют «зомби», поскольку они действуют по чужому приказу. Компьютер может быть заражен через браузеры при посещении различных зараженных сайтов, при получении почты или при установке нелицензионного программного обеспечения. «Зомби» зачастую невидимы файерволу или неотличимы от реального пользователя, что также усложняет борьбу с ними.

Впервые о Ddos-атаках стало известно в 1996 году, однако серьезную проблему они начали представлять через три года, когда хакерам удалось вывести из строя сайты таких компаний как Amazon, Yahoo, CNN, eBay и некоторых других. На сегодняшний день заказать такую атаку довольно просто и относительно недорого. Разумеется, разрушение корпоративного сайта — неблагоприятное событие. Однако оно становится полностью катастрофичным, если от работы портала напрямую зависит прибыль компании или если атака

происходит во время проведения грамотной, продуманной, хорошо спланированной и оплаченной интернет-кампании по продвижению и раскрутке.

В настоящее время чаще всего при проведении атаки используется трехуровневая структура. Верхний уровень занимает управляющий компьютер (или несколько компьютеров), с которого подаются управляющие сигналы — в том числе и о начале атаки. Следующими в ряду идут управляющие консоли, через которые сигналы распределяются по миллионам компьютеров пользователей. Именно эти, находящиеся в самом низу «безгласные исполнители» и отправляют запросы на интернет-узел, являющийся целью преступников. Проследить обратную связь невозможно, максимум — можно вычислить одну из управляющих консолей, которые также, кстати, считаются пострадавшими от атаки.

Сложностью в выявлении преступников является и свободное распространение в сети программ для проведения атак. Изначально подобное программное обеспечение разрабатывалось для выявления степени устойчивости сети к внешним нагрузкам. Однако за годы оно претерпело сильные изменения, было сформировано и усовершенствовано несколько видов атак, которые к тому же могут сочетаться, варьироваться и видоизменяться. Именно поэтому защита от Ddos - атак должна быть профессиональной, постоянной и обновляемой.

Технологии проведения DoS и DDoS атак разнообразны, от простого навала на ресурс, до техники "умного" DoSa, атакующего конкретные слабые, или долго выполняющиеся скрипты сайта.
Часто злоумышленники пользуются уязвимостями в серверном программном обеспечении. Старые версии серверного ПО подвержены множественным уязвимостям, включая неустойчивостью к DoS и DDoS атакам. Применяются эксплойты использующие эти уязвимости, для организации DoS и DDoS атак.
Техникой "умного" DDoSa так же является атака, приводящая к отказу в

обслуживании путем превышения лимитов установленных хостинг - провайдерами.

Практически у всех хостингов существуют недокументированные ограничения в обслуживание, такие как количество единовременных обращений к файловой системе сервера, ограничение по нагрузке на процессор и т.п. Обладая этой информацией злоумышленник направляет атаку на сайт или сервер целью которой является превышение этих лимитов.

DDoS-атака – аббревиатура от английского Distributed Denial of Service, распределенная атака, направленная на отказ в обслуживании. Атаки такого типа могут быстро истощить сетевые ресурсы или мощности сервера, что приведет к невозможности получить доступ к ресурсу и вызовет серию негативных последствий: упущенная прибыль, невозможность воспользоваться услугами и произвести различные транзакции и т.д. В DDoS-атаке в роли атакующего выступает так называемая бот-сеть, или зомби-сеть. Зомби-сеть может насчитывать от нескольких десятков до тысяч хостов. Обычно это нейтральные компьютеры, которые в силу каких-то причин (отсутствие файрвола, устаревшие базы антивируса и т.д.) были заражены, вредоносными программами. Программы, работая в фоновом режиме, непрерывно посылают запросы на атакуемый сервер, выводя его таким образом из строя [2].

В настоящий момент не существует какого-то универсального средства для противодействия DDoS-атакам. Даже такие крупные компании, как Microsoft, eBay, Amazon, Yahoo, страдают от DDoS-атак и не всегда могут с ними справиться. Чаще всего атаке подвергаются сайты, созданные для того, чтобы зарабатывать деньги. Для интернет-магазина простой в несколько часов — убытки из-за полного отсутствия заказов и прибыли.

Вывод из строя сайта даже на небольшой промежуток времени может сказываться не только на показателях, но и на количестве пользователей. К

примеру, отсутствие доступа на крупном проекте с многомиллионной посещаемостью даже на несколько часов вполне может означать отток пользователей на конкурирующие проекты (с учетом, промежутка времени, в основном это коснется пользователей, относительно недавно начавших использовать ресурс).

Несмотря на то, что достаточно часто атаки Отказ в обслуживании (DoS) и ее распределенный вариант (DDoS) проводятся на небольшие или средние сайты, все же крупные порталы так же подвергаются данным атакам и, порой, весьма успешно.

1.2 Анализ существующих типов DDoS-атак

Для ИТ-службы атака DDoS является серьезным испытанием — нужно выявить источник атаки, выяснить ее природу и выработать механизмы защиты. При этом средства защиты должны блокировать непродуктивные запросы, инициированные нападающими и не приносящие компании доходов.

Все DDoS атаки можно разделить на три обширные группы:

- объёмные;
- атаки на уровне протоколов;
- атаки на уровне приложений.

Подробнее отдельные виды атак будут рассмотрены ниже, а пока — небольшой обзор групп.

Атаки, направленные на объём.

Данная категория атак направлена на насыщение полосы пропускания, соответственно, сила атаки измеряется в битах в секунду. К этой категории разносятся различные виды флудов: UDP, ICMP и прочие потоки сфальсифицированных пакетов. Сила атаки растёт с каждым годом, и если в далёком 2002 году 400 Мбит/с казалось чем-то из ряда вон выходящим, то сейчас

отдельные атаки превышают 100 Гбит/с и способны «сдуть» некоторые «карманные» дата-центры. Пожалуй, единственный способ борьбы с такими атаками — фильтрация на уровне дата-центра (если он предоставляет такую услугу) или специализированных сервисов защиты. Они обладают достаточными канальными мощностями и вычислительными ресурсами, чтобы поглотить объём и передать на сервер пользователя уже отфильтрованный трафик. Для «выщипывания» остатков паразитного трафика можно также применить средства аппаратной защиты.

Атаки на уровне протоколов.

Эта категория направлена на ограничения оборудования или уязвимости различных протоколов. Такие атаки забивают ресурсы сервера либо промежуточного оборудования (фаерволы, балансировщики нагрузки и т.п.) паразитными пакетами, в результате чего системы оказываются неспособны обрабатывать полезные. Сила атаки измеряется в пакетах в секунду. К этой категории относятся SYN флуд, атаки с фрагментированными пакетами и другие. На этом уровне аппаратная защита становится ощутимо эффективнее. Специально разработанные производителями таких устройств алгоритмы помогают отсортировать и отфильтровать трафик. Естественно, любые алгоритмы несовершенны, и какая-то часть паразитного трафика всё-таки прорвётся, а какая-то часть полезного может быть утеряна. Сторонние сервисы фильтрации также могут быть вполне эффективны.

Атаки на уровне приложений.

Как можно понять из названия0ёаки направлены на уязвимости в приложениях и операционных системах (Apache, Windows, OpenBSD и т.п.). Они приводят к неработоспособности какого-либо приложения или ОС в целом. Среди таких атак: Slowloris, атаки нулевого дня и прочие. Как правило, состоящие из

вполне невинных свиду запросов, такие атаки выводят из строя веб-сервер. Интенсивность измеряется в запросах в секунду.

Данный тип атак наиболее «убийственный». Они чрезвычайно узко направлены, благодаря чему могут создать весьма серьёзные проблемы атакуемому при малых затратах ресурсов атакующего. За последние 3-4 года данный тип атак становится преобладающим, и простой флуд HTTP GET запросов является одним из наиболее распространённых видов.
К арсеналу борьбы с этой категорией атак, помимо упомянутых выше внешних сервисов и аппаратной защиты, можно также добавить встроенные программные алгоритмы, анализирующие запросы и создающие правила для фаервола по результатам такого анализа.

DDoS атаки уровня приложений

Этот вид атак основан на использовании уязвимостей различных операционных систем и приложений (Apache, Windows, OpenBSD). На работу ресурса они влияют опосредованно, но от этого не менее эффективно – в случае отказа важного приложения или всей системы вцелом, ресурс или его часть становятся недоступными и не отвечают на запросы пользователей. Эффективность таких атак очень высока, а отследить их чрезвычайно сложно благодаря «точечному» воздействию. Кроме того, они не требуют большого количества ресурсов для своей реализации.

Уровень воздействия для атак из этой категории измеряется в количестве запросов за единицу времени.

Например, Slowloris (один из видов атак на веб-сервера), способен «завесить» сервер благодаря использованию уязвимости в его архитектуре (актуально для Apache первой и второй версии, Squid, dhttpd, и GoAhead WebServer). Веб-серверы на основе Apache имеют ограничение по количеству открытых подключений. Бомбардируя сервер большим количеством пакетов

данных с определенной периодичностью, хакер может «завесить» его на неопределённое время. Причем уровень загрузки процессора в данном случае будет относительно невысоким – сервер просто будет бесконечно ожидать закрытия активных подключений. Для проведения атаки такого уровня будет достаточно одного среднестатистического ПК с определенным набором программ. Использование последних версий Apache, где эта уязвимость устранена, или организация работы сервера на базе lighttpd позволит не переживать по поводу работы Slowloris. Данный пример здесь присутствует только для ознакомления с механизмом воздействия, потому что производители программных продуктов стараются оперативно реагировать на выкладываемую в сети информацию. И при выявлении подобного рода уязвимостей – выпускать так называемые «заглушки», предохраняющие от хакерских атак, в кратчайшие сроки. Чтобы защититься от DDoS атак на уровне приложений, необходимо предусмотреть фильтрацию входящего трафика, как на уровне сервера, так и с привлечением сторонних ресурсов.

SYN флуд, icmp flood и другие DDoS атаки уровня протоколов.

Уже из названия понятно, что уязвимость ищется в протоколах, по которым работает сервер. Атаки подобного рода ориентированы на поглощение ресурсов сервера или промежуточных серверов (оборудования). Суть действий злоумышленников проста – пока обрабатываются пакеты, отправленные хакером, пакеты от пользователей ждут своей очереди. Если количество отправленных злоумышленниками пактов значительно превысит количество пакетов от обычных пользователей, время ожидания ответа от сервера у пользователей станет непозволительно большим.

Наиболее распространёнными примерами таких атак пинг смерти, SYN флуд, icmp flood и другие. Уровень воздействия здесь измеряется в количестве пакетов на единицу времени. Для защиты от нападений подобного рода подходят

различные алгоритм фильтрации входящего трафика на аппаратном уровне. Еще один вариант – воспользоваться услугами специальных сервисов, специализирующихся на фильтрации трафика от «флуда»

Атака udp flood в сегменте объемных DDoS

Этот тип атак направлен на превышение пропускной способности канала. Примерами атак этого вида относятся различные виды «флудов»: SYN, UDP, ICMP, MAC и другие. Например, атака udp flood. Для нее характерна бомбардировка портов удаленного хоста большим количеством UDP - пакетов. Так как в протоколе UDP не предусмотрена защита от перегрузок, трафик от злоумышленника постепенно вытесняет запросы от обычных пользователей. Сохранить анонимность атакующих хостов можно, подменив IP-адреса источников, указанные в UDP – пакетах.

Возможности злоумышленников растут соизмеримо с развитием технологий. Если в 2002 году атака со скоростью 400Мбит/с считалась практически непреодолимой, то современные дата-центры подвергаются атаками со скоростью до 100Гбит/с. Эффективность объёмной DDoS атаки измеряется в количестве бит за единицу времени.

Наиболее эффективным способом защиты от нападений подобного рода – использование специализированных фильтров на уровне дата-центров или сторонних сервисов, предоставляющих такие услуги.

1.3 Виды DDoS атак в классификации по уровням OSI

OSI – семиуровневая эталонная модель, описывающая схему взаимодействия сетевых устройств. Модель OSI была разработана еще в 70-х годах, и описывала взаимодействие семейства собственных протоколов, которые разрабатывались как главные конкуренты TCP/IP. И хотя особого распространения они так и не получили, модель взаимодействия оказалась настолько удачной, что стала применяться для TCP/IP протоколов как тогда, так

и сейчас. Виды DDoS атак и защит от них, доступных на каждом из уровней, различны.

1 уровень. Физический.

Этот уровень специализируется на передаче потока данных в двоичном коде по протоколам 100BaseT, 1000 Base-X. Результатом воздействия DDoS атаки на этом уровне будет разрушение или невозможность управления (на физическом уровне) концентраторов или патч-панелей, использующих описанные выше протоколы. Для восстановления работы оборудования в штатном режиме потребуется его полноценный ремонт. В качестве профилактических действий, способных защитить негативных последствий нападений злоумышленников на этом уровне, можно порекомендовать систематически проверять состояние оборудования.

Применительно к беспроводным сетям, DDoS атаки на физическом уровне характеризуются генерацией различного вида помех, способных нарушить связи между элементами сети.

2 уровень. Канальный.

Отвечает за взаимодействие элементов сети на физическом уровне, оперируя кадрами по протоколам 802.3 и 802.5 посредством котроллеров, точек доступа и мостов, их использующих. Примером DDoS атаки на этом уровне является MAC-флуд – переполнение коммутаторов пакетами данных, которое влечет за собой блокирование их портов. Для избегания подобных проблем рекомендуется использовать современное сетевое оборудование – во многих моделях предусмотрена функция сохранения надежных MAC адресов, прошедших аутентификацию. Таким образом, можно ограничить и отфильтровать запросы в соответствии с настройками оборудования, отсекая ненадежные или «флудящие» адреса.

3 уровень. Сетевой.

На этом уровне происходит маршрутизация и обмен данными между сетями посредством передачи пакетов с информацией по таким протоколам IP, ICMP, ARP, RIP. Примером DDoS атаки на этом уровне является ICMP-флуд. Суть атаки состоит в том, что хост постоянно «пингуется» нарушителями, вынуждая его отвечать на ping-запросы. Когда их приходит значительное количество, пропускной способности сети не хватает, и ответы на запросы приходят со значительной задержкой. Для предотвращения таких DDoS атак можно полностью отключить обработку ICMP запросов посредством Firewall, или хотя бы ограничить их количество, пропускаемое на сервер.

4 уровень. Транспортный.

Назначение этого уровня – обеспечение стабильной и безошибочной передачи данных между узловыми точками сети. Кроме того, именно на этом уровне происходит управление процессом передачи информации с физического на сетевой уровень. Осуществляется по протоколам TCP и UDP.

Виды DDoS атак, применяемые на этом уровне - SYN-флуд, Smurf-атака и другие. В результате таких атак наблюдается превышение количества доступных подключений (ширина канала достигает своего предела), и возможны перебои в работе сетевого оборудования. Самым распространенным методом противодействия таким атакам является blackholing. Это метод фильтрации трафика на уровне провайдера, до его попадания в частные сети. Его суть состоит в том, что в случае атаки сетевой администратор сможет настроить систему таким образом, чтоб пакеты от злоумышленников будут отбрасываться. У blackholing есть и минусы – при недостаточно точных параметрах фильтрации, кроме вредоносных пакетов, могут отсекаться и запросы от «легальных» пользователей, не имеющих к злоумышленникам никакого отношения.

5 уровень. Сеансовый.

На этом уровне происходит инициализация процессов установки и завершения сеансов связи в рамках ОС (например, при смене пользователей в windows), а так же их синхронизация в рамках одной сети посредством протоколов протоколы RPC, PAP. На этом уровне атакам подвергается сетевое оборудование. Используя уязвимости программного обеспечения Telnet-сервера на свитче, злоумышленники могут заблокировать возможность управления свитчем для администратора. Чтоб избежать подобных видов атак, необходимо поддерживать прошивки оборудования в актуальном состоянии. Для предотвращения использования «дыр» в программном обеспечении в будущем, после каждой успешной атаки производитель в обязательно порядке выпускает «заглушку». Использование только актуального лицензионного ПО на серверах снижает значительно уровень угроз на сеансовом уровне.

6 уровень. Представления.

На этом уровне происходит передача данных от источника к получателю. Используются протоколы ASCII, EBCDIC, направленные на сжатие и кодирование данных. Наиболее часто для атак на этом уровне используется технология подложных SSL запросов. Так как для проверки зашифрованных пакетов SSL затрачивается значительное количество ресурсов, зачастую их расшифровка происходит уже внутри сети организации или на сервере ресурса. Другими словами, чтобы не тратить значительное время на расшифровку шифрованных запросов, фаерволл и другие системы безопасности просто пропускают их без проверки дальше по сети. Этим часто пользуются хакеры, генерируя собственные подложные SSL запросы, которые могут инициировать самовольную перезагрузку сервисов, ответственных за прием SSL соединений.

Еще одним моментом, работающим на руку злоумышленникам, является тот факт, что процесс расшифровки пакета требует практически в 10 раз больше ресурсов, чем необходимо для зашифровки. Атаки, производимы посредством

подложных SSL запросов, могут принести значительный вред, при этом ресурсные затраты злоумышленника будут относительно невелики. Подходить к защите от DDoS атак на этом уровне следует комплексно: использовать специализированные средства, проверяющие входящий трафик (фильтрация трафика DDoS), и попытаться распределить инфраструктуру SSL (например, разместить функционал SSL – терминирования на отдельном сервере).

7 уровень. Приложений.

На этом уровне происходит оперирование данными посредством пользовательских протоколов (FTP, HTTP, POP3,SMTP, Telnet, RAS). Следствием DDoS атак здесь становится тотальная нехватка ресурсов для выполнения простейших операций на подвергшемся атак ресурсе. Наиболее эффективным способом противодействия злоумышленникам – постоянный мониторинг состояния системы в целом и программного обеспечения в частности. После выявления атаки на этом уровне можно идентифицировать злоумышленника и полностью заблокировать возможность совершения им каких-либо действий.

1.4 Обнаружение вторжений и вредоносного программного обеспечения

В этом разделе рассмотрены существующие методы обнаружения атак; определены, почему эти методы не достаточны для обнаружения; описаны сходства и различия рассмотренных методов и предлагаемого в работе решения. В частности, для сравнения существующих решений описывается таксономия методов обнаружения сетевых атак направленных на отказ в обслуживаний.

Существующие техники обнаружения вторжений и вредоносного программного обеспечения (далее –ВПО) можно классифицировать на сетевые решения и решения, функционирующие на узлах. Используемые на узлах техники обнаружения очень важны для распознавания исполняемых файлов ВПО и аномалии в поведении на уровне узла (например, вызывается определенный

системный вызов и создаются определенные ключи реестра). Антивирусные инструменты полезны для традиционного обнаружения вирусов в течение длительного времени[7]. Другой типичный пример метода обнаружения вторжения на основе узла–это мониторинг системных вызовов[11].

Но когда встает проблема обнаружения ботнетов, эти методы обнаружения, основанные исключительно на анализе узла, имеют некоторые проблемы. Во-первых, традиционные антивирусные инструменты основаны на поиске сигнатур, таким образом, требуют объемной, точной и часто обновляемой базы сигнатур. Ботнеты могут легко избежать сигнатурного обнаружения, обновляя себя чаще, чем пользователи обновляют свои антивирусные базы. Во-вторых, системы обнаружения на основе узла находятся на том же уровне привилегий, что и боты на некотором узле. Таким образом, боты могут отключить антивирусные средства системы или использовать руткит-технологии, чтобы защитить себя от обнаружения на локальном узле. Частота обнаружения ботов относительно низка по сравнению с традиционными вредоносными программами. Например, вредоносное программное обеспечение Kraken было не замечено 80% коммерческих антивирусных средств. Проведенное в PandaLabs в 2007 году исследование установило, что даже при установленной актуальной защите (например, антивирусные средства) значительная часть персональных компьютеров (22,97%) заразились вредоносными программами. Таким образом, миллионы узлов Интернета связаны с деятельностью ботнетов [15], а фактический процент может быть еще выше. Кроме того, мониторинг узла в реальном времени на основе поведения, как правило, сопровождается значительными накладными расходами системы, за счет чего такие решения могут стать менее привлекательными для конечных пользователей. Таким образом, в рамках работы акцент делается на сетевые решения обнаружения. Оставшаяся часть этого раздела будет сфокусирована на работах,

соответствующих исследованию, главным образом, основанных на сети. Существующие исследования проблемы обнаружений вторжений, основанных на сети, предложили немало методов и систем обнаружения вторжений. Snort [12] и Bro [44]–пара представителей систем обнаружения вторжений (далее-СОВ),основанных на сигнатурах. Они полагаются на большую базу сигнатур для идентификации попыток вторжения в сетевом трафике. Основной недостаток сигнатурных СОВ похож на недостаток антивирусных средств–это невозможность определять новые атаки, потому что они ранее ни когда не встречались и, соответственно, не имеют сигнатур. СОВ, основанные на анализе аномалий, могут преодолеть это ограничение путем описания нормального, легитимного трафика. Соответственно, любое отклонение от этого описания будет считаться аномалией. Примерами таких систем являются PAYL[42] и Anagram [41]. Эти системы изучают полезную нагрузку входящих пакетов, проводят n-граммный анализ и выявляют эксплойт в полезной нагрузке. Основной недостаток решений на основе анализа аномалий –это большое количество ложных срабатываний. До распространения ботнетов типичным вредоносным программным обеспечением являлись черви. Червь –это само распространяющаяся вредоносная программа, которая копирует себя, используя сетевые технологии. Основным отличием ботнета от червей является наличие управляющего канала. Поэтому ботнеты являются более гибкими, чем черви. Гибкость заключается в возможности управления деятельностью ботов, в то время, как деятельность червей запрограммирована разработчиком заранее и отсутствует возможность выбирать функциональность червя после заражения.

Компания Cisco, лидер в производстве и реализации сетевых решений, признает, что на сегодняшний день нет достаточных средств для борьбы с DDOS атаками. Это связано с тем, что атаки такого типа возникают неожиданно и у системных администраторов нет возможности проанализировать атаку до

момента ее начала. Подбирать меры противодействия атакам приходится уже в момент проведения атаки, когда сетевой ресурс уже испытывает трудности. Кроме того, в каждом конкретном случае опыт прошлых атак может быть недостаточен для отражения новой атаки. Это связано с тем, что злоумышленники постоянно развивают средства атак, меняют стиль, конфигурацию пакетов и т.д.. Исследование DDOS атак сходно с изучением природных явлений, таких как землетрясения, извержения вулканов, разряды молнии, т.е. которые могут быть напрямую исследованы только в момент их наступления. Можно создать математическую или компьютерную модель DDOS атаки и проводить ее исследования, но нет никаких гарантий, что эта модель будет отображать все нюансы следующей DDOS атаки, которую смогут придумать и реализовать злоумышленники. Аналогично и со средствами защиты, злоумышленник может найти элемент сетевого ресурса, атака на который приведет к отказу в обслуживании всего ресурса. Для исследования DDOS атак необходим механизм, который бы в лабораторных условиях мог повторять реальные DDOS атаки сколь угодное количество раз, эмулировать новые атаки, максимально соответствующие реальным, вносить изменения в основные параметры атаки и отслеживать результат. По своей сути механизм должен представлять распределенную зомби-сеть, максимально приближенную к реальным действующим бот-сетям.

Методы защиты от DDoS-атак можно условно классифицировать по двум признакам. Первый признак – расположение механизма защиты в сети. Методы защиты могут подразделяться на применяемые у источника, на стороне жертвы, а также на промежуточных узлах сети. Методы, объединяющие различные схемы защиты и обеспечивающие их взаимодействие, обычно называют гибридными [14]. Принято считать, что гибридные методы обеспечивают лучшую защиту от атак, нежели отдельные методы защиты, работающие самостоятельно на

различных участках сети. Второй признак – время применения метода. Механизмы, применяемые до наступления атаки, относятся к методам предотвращения [7]. Методы, используемые во время атаки, относятся к группе обнаружения атаки и идентификации источника. После обнаружения атаки применяются методы реакции на атаку. Наилучшим вариантом является предотвращение атаки. Оно может быть достигнуто на всех этапах пути трафика, начиная от источника атаки и заканчивая обработкой данных на стороне атакуемого сервера. Зачастую используются комбинированные средства предотвращения (IPS) и обнаружения атак (IDS) – IPDS.

Методы, основанные на механизмах фильтрации

Существует множество методов предотвращения DDoS-атак. Для этого очень часто исследователи предлагают различные механизмы фильтрации, например Ingress/Egress filtering [8] , SAVE [9], Hop-Count filtering [10], Route-based filtering [11] и др. Фильтрация является весьма эффективным способом выявления подмены IPадреса, что особенно актуально в тех случаях, когда используется усиление или отражение атаки. Различные методы фильтрации, применяемые на разных этапах продвижения трафика, представляют собой мощный инструмент для выявления фактов подмены адреса. Наибольшее распространение получил метод Ingress/Egress filtering, так как он позволяет выявить подмену IP-адреса и заблокировать вредоносный пакет еще до того, как он покинет локальную сеть. На основе методов фильтрации трафика были созданы более сложные гибридные механизмы защиты, такие, как TRACK [12], Active Internet Traffic Filtering (AITF) [13], StopIt [14] и др. Эти методы выявляют вредоносный трафик и отправляют на маршрутизаторы запросы на фильтрацию пакетов от подозрительного источника. Каждый из этих методов применяет различные схемы обнаружения вредоносного трафика и различные методы фильтрации. Однако не все методы ориентированы на случаи подмены адреса.

Так, например, метод StopIt применяет фильтрацию на ближайшем к источнику трафика маршрутизаторе. При этом реальный путь трафика не отслеживается, и запрос на блокировку поступает к источнику, адрес которого указан в подозрительном пакете в качестве адреса отправителя. В том случае, если использовалась подмена адреса, будет осуществляться фильтрация от источника, который на самом деле может быть легитимным пользователем. Таким образом, следует уделять внимание проблеме подмены адреса и тем способам фильтрации и отслеживания реального пути трафика, которые позволяют ее выявить. Тем не менее, данные методы можно успешно использовать в составе комплексных решений по противодействию атакам.

Математические методы и методы интеллектуального анализа данных Помимо уже описанных методов для анализа трафика могут быть реализованы механизмы защиты на основе математических методов, например определение энтропии [15]. В последние годы активно разрабатываются методы защиты, основанные на различных алгоритмах интеллектуального анализа данных. В качестве примеров можно привести механизмы на основе метода ближайших соседей (kNN) [16], обучаемых нейронных сетей [17]. Такие методы могут быть применимы и для противодействия атакам, использующим отражение трафика и его усиление. Интеллектуальные способы анализа данных позволяют выявить различные девиации трафика, а также подозрительное поведение клиентов. Сложность заключается в том, что обучение нейронных сетей, например, может занять весьма продолжительное время. В работе [18] была предложена статистическая модель обнаружения DDoS-атак, осуществляемых по протоколу TCP. Модель анализирует флаги в заголовке каждого пакета и сравнивает реальный трафик с заданным шаблоном нормального трафика. Отклонения от шаблонного трафика расцениваются как аномалия. Метод, представленный в работе [19], основан на принципе асимметрии трафика в случае

атаки. В качестве шаблона нормального трафика принята схема симметричного обмена запросами клиента и ответами сервера. В случае значительного повышения количества входящих запросов или ответов на запросы, которые не могут быть корректно обработаны, нарушается симметрия трафика, и такая ситуация расценивается как атака. Стоит отметить, что анализ симметричности трафика предлагается также в качестве метода борьбы с атаками, основанными на отражении трафика и его усилении, так как при данных атаках асимметрия трафика является значительной и такую атаку становится легко выявить. Метод защиты одноранговых сетей от различных атак, направленных на инфраструктуру компьютерной сети, представлен в работе [20]. Предлагаемый механизм защиты устанавливается на пограничном маршрутизаторе сети, на которую направлена атака. Метод обнаружения атаки основан на статистическом анализе трафика и его сопоставлении с шаблонным трафиком. После обнаружения атаки используется схема маркировки пакетов с целью выявления источника атаки и блокировки трафика от него. Такая схема представляет собой один из эффективных методов защиты и в случае, когда используется под- мена адреса, так как отслеживается реальный путь трафика, а не выполняется блокировка трафика от указанного в пакете отправителя.

Механизмы защиты от атак, использующих отражение трафика. Рассмотрим механизмы защиты, разработанные непосредственно для атак, основанных на отражении и усилении трафика. Общий механизм предотвращения отражения трафика RAD (Reflector Attack Defense) предлагается в [21]. В основе метода используется message authentication code (MAC). Когда тот или иной узел отправляет запрос, он помещает MAC в отведенное поле. В ответе на это сообщение размещается тот же самый MAC, что и в запросе. Узел, получив ответ на запрос, сверяет MAC из отправленного им запроса и MAC из полученного ответа. Если MAC совпадают, сообщение принимается. В противном случае

считается, что ответ представляет собой отраженный трафик и сообщение отклоняется. В настоящее время разработано множество методов защиты от DNS-атак. В работе [22] в основе метода защиты DAAD (DNS Amplification Attacks Detector) лежит тот факт, что при атаке DNS атакуемый узел получает большое количество ответов на отправленные ранее запросы. Авторы предлагают вести базу адресов DNS-серверов, на которые отправлялись запросы от того или иного узла. Все получаемые ответы должны проверяться, и если входящий пакет действительно является ответом на запрос, он будет принят. Если же с узла, которому адресован ответ, не отправлялся DNS-запрос на данный сервер, такой пакет должен быть отклонен. Данный метод весьма эффективен, однако следует помнить, что ведение подобных баз требует большого объема ресурсов. В работе [23] предлагается установка предварительного DNS-резольвера и создание туннеля, использующего протоколы IPSec или SSL, между предварительным резольвером и DNS-резольвером на стороне организации. Все запросы DNS проходят исключительно через туннелированный канал связи и не могут поступить напрямую из внешних источников. Отмечается, что основная фильтрация DNS-ответов должна осуществляться провайдером услуг интернет-связи после соответствующего запроса от организации. Туннелирование в данном случае играет лишь вспомогательную роль. В работе [24] предлагается механизм RRL (Response Rate Limiting), направленный на ограничение числа уникальных ответов от DNS-сервера. Этот механизм защиты используется на стороне DNS-сервера и анализирует исключительно исходящий трафик, полностью игнорируя входящий. Суть метода заключается в том, что адреса, на которые был отправлен ответ, записываются. При этом задается ограничение числа ответов сервера на каждый адрес. Если это число превышено, ответы на данный адрес больше не высылаются. Такой метод эффективен для снижения потока вредоносного трафика от сервера, но при этом существует вероятность ошибки первого рода. В

работе [25] предлагается метод FB (Flowbased), основанный на выявлении девиации трафика относительно шаблонного. Анализируется количество входящих пакетов по протоколу DNS и их размер. Если количество и размер пакетов превышают заданные значения, такая ситуация расценивается как атака. При этом автор отмечает, что в ситуациях, когда осуществляется атака, но при этом анализируемые параметры не превышают пороговых значений, трафик считается легитимным. Таким образом, процент ошибок второго рода в отдельных случаях может быть весьма высок. Данный метод, тем не менее, весьма перспективен при соответствующей доработке. Следует отметить, что рассмотренные методы были разработаны для противодействия атакам, реализуемым с помощью протокола DNS. Что касается атак, реализуемых по другим рассмотренным протоколам, то, например, основным средством предотвращения популярных в последние несколько лет атак по протоколу NTP является отключение команды мониторинга на стороне серверов. В настоящее время данную уязвимость имеют версии ntpd до 4.2.7p25 включительно, в выпуске 4.2.7p26 и выше команда monlist отключена. Иных мер, направленных на борьбу с отраженным трафиком, поступающим по протоколу NTP, до настоящего времени не предлагалось. В целом, в качестве основной меры борьбы с атаками, основанными на отражении, рекомендуется отключать те функции серверов, которые могут использоваться для реализации атак, а также закрывать неиспользуемые порты. Такое решение, на первый взгляд, кажется самым простым и действенным, однако не все владельцы серверов по тем или иным причинам следуют этой рекомендации. Применительно к устройствам, принадлежащим пользователям, решить эту проблему становится сложнее. Статистика проведенных атак свидетельствует о том, что популярные типы атак, основанных на отражении, по- прежнему легко реализовать. Несмотря на то, что, например, поддержка команды get_monlist была отключена в новых версиях

протокола NTP, атаки данного типа продолжают занимать одну из лидирующих позиций. Это свидетельствует, в том числе, и о том, что не все владельцы NTP-серверов обновляют версии протокола до более безопасных, а значит, не все заботятся о предотвращении атак, в которые могут быть вовлечены их серверы. В статье были рассмотрены протоколы, которые могут использоваться для реализации отражения трафика и его усиления. Проведенный анализ показал, что достаточно большое количество протоколов, основанных на протоколе UDP, имеют те или иные уязвимости, позволяющие реализовать отражение трафика. Растущая мощность атак, основанных на усилении трафика, а также количество таких атак свидетельствуют о том, что необходима разработка новых эффективных средств защиты компьютерных сетей. Остается нерешенной проблема фильтрации исходящего трафика на стороне сервис- провайдеров, что по-прежнему делает возможной подмену адреса источника. Многообразие протоколов, которые могут быть использованы для реализации атак, показывает необходимость поиска универсальных методов обнаружения возможных атак, использующих отражение и усиление. Не следует забывать о том, что потенциально опасные протоколы, на сегодняшний день находящиеся в тени, в ближайшем будущем могут стать инструментом для реализации массированных атак. Таким образом, следует не только уделить внимание уязвимостям, присущим популярным в настоящее время протоколам, но и разработать схемы противодействия как существующим, так и потенциально возможным атакам. В качестве дальнейшей цели ставится задача проведения серии экспериментов по оценке эффективности существующих методов защиты для атак с различными сценариями.

Выводы по первой главе

Целью диссертационной работы является повышение защищенности информационных систем от DDoS атак с на основе разработки и применения системы обнаружения и блокирования вредоносного трафика с использованием алгоритмов интеллектуального анализа данных. Для достижения цели в работе были сформулированы и решены следующие задачи:

1. Исследовать распространенные атаки типа «отказ в обслуживании», процесс их реализации и механизмы защиты от них, проанализировать существующие подходы к выявлению атак.
2. Разработать алгоритм обнаружения управляющего трафика в глобальных сетях с использованием технологий интеллектуального анализа данных.
3. Предложить архитектуру системы обнаружения и блокирования ботнетов, проанализировать эффективность функционирования предложенных в диссертационном исследовании алгоритмов.
4. Разработать метод распределенного обнаружения управляющих компонент ботнета, позволяющий обнаруживать управляющие серверы и узлы сети, с которых осуществляется контроль атаки, основанный на сигнатуре управляющего трафика.
5. Разработать программную систему для обнаружения и блокирования DDoS атак, дать рекомендации по практическому внедрению разрабатывающей системы обнаружения и блокирования вредоносного трафика.

ГЛАВА 2 АНАЛИЗ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ

2.1 Решения, представляемые компанией Arbor

Сегодня DDoS-атаки являются одним из наиболее доступных и эффективных инструментов, позволяющих преступникам препятствовать деятельности или полностью блокировать web-сайты организаций и каналы связи провайдеров. Информация о резонансных DDoS-атаках на правительственные сайты разных стран, блогохостинги, сетевые средства массовой информации, Интернет-магазины и торговые площадки периодически появляется в новостных лентах. Безусловным мировым лидером по производству решений, с помощью которых осуществляется защита от DDoS-атак, является компания Arbor Networks. Компания производит системы защиты от DDoS-атак двух классов: решения для операторов связи Arbor Peakflow SP и решения для предприятий различного уровня и Интернет-площадок Arbor Pravail.

Arbor Peakflow SP

Защита от DDoS атак, построенная на применении решений Arbor Peakflow SP, используются у большей части магистральных и средних провайдеров во всём мире, в том числе и в России. Система состоит из нескольких типов устройств: Peakflow CP, Peakflow TMS, Peakflow FS, Peakflow PI, Peakflow BI, но базовая инсталляция системы обычно включает только первые два типа.

Peakflow CP является основным компонентом системы защиты – этот сервер является центром управления системой защиты и центром мониторинга всей сети провайдера. На Peakflow CP поступает информация о сетевом трафике и маршрутизации в сети, а также о состоянии и загрузке маршрутизаторов. Устройство Peakflow TMS является интеллектуальным сетевым экраном – трафик, содержащий атаку, фильтруется на серверах TMS. При этом TMS может стоять

либо в разрыве канала связи, либо «в стороне», в последнем случае зараженный трафик перенаправляется на TMS для очистки с использованием динамической маршрутизации BGP.

Система Arbor Peakflow SP содержит огромное количество настраиваемых шаблонов и контрмер, посредством которых обеспечивается не только эффективная защита от ддос атак, но и вообще гибко фильтруется трафик по самым разным признакам: по URL-адресам, по географическому расположению - страна, регион, населенный пункт, по структуре IP-пакетов, по характеру и структуре трафика, и т.д. Система также предоставляет портальный интерфейс – возможность создания «личных кабинетов» для клиентов оператора связи. В «личном кабинете» клиент имеет доступ ко всей информации, относящейся к его защищаемым ресурсам - мониторинг, статистика, информация об атаках и прочее, а также возможность самостоятельно управлять защитой своих ресурсов.

В Arbor Networks функционирует специализированная сетевая лаборатория ASERT (Arbor Security Engineering and Response Team), в задачи которой входят постоянный мониторинг и анализ аномалий и DDoS-атак в сетях операторов связи по всему миру, поддержание базы знаний об атаках и ботнетах, использование этих сведений для эффективного обнаружения и подавления атак системами Arbor. Благодаря механизму обмена информацией Fingerprint Sharing Alliance на все устройства Arbor оперативно доставляется актуальная информация и новые сигнатуры.

Arbor Pravail

Решения Arbor Pravail предназначены для организаций различного уровня и Интернет-площадок, для которых актуальна задача защиты от DDoS атак и обеспечения непрерывного функционирования своих Интернет-сайтов и

порталов. Arbor Pravail является первым полноценным решением на рынке ИБ в своем классе (защита от DDoS для предприятий, а не провайдеров), был представлен на рынке относительно недавно (в 2011 г.) и аккумулирует в себе весь опыт и технологии Arbor Networks по защите от DDoS-атак, которые производитель накопил за много лет.

Система представляет собой единый аппаратно-программный комплекс, устанавливаемый на внешнем периметре организации между корпоративным межсетевым экраном и операторами связи. Arbor Pravail использует сигнатурный и поведенческий методы анализа для обнаружения атак, позволяет осуществлять их подавление в автоматическом и полуавтоматическом режимах. Системы Arbor Pravail подключены к лаборатории ASERT, что обеспечивает доступ к наиболее полной и актуальной базе знаний о ботнетах и особенностях DDoS-атак, и как следствие – возможности эффективного обнаружения и подавления.

2.2 Средства защиты от DDoS-атак, предоставляемые провайдером

Проектирование, развертывание и эксплуатации глобальной Anycast-сети требует времени, денег и ноу-хау. Большинство ИТ-организаций не располагают для этого специалистами и финансами. Можно доверить обеспечение функционирования инфраструктуры DNS провайдеру – поставщику управляемых услуг, который специализируется на DNS. Они имеют необходимые знания для защиты DNS от DDoS-атак.

Поставщики услуг Managed DNS эксплуатируют крупномасштабные Anycast-сети и имеют точки присутствия по всему миру. Эксперты по безопасности сети осуществляют мониторинг сети в режиме 24/7/365 и применяют специальные средства для смягчения последствий DDoS-атак.

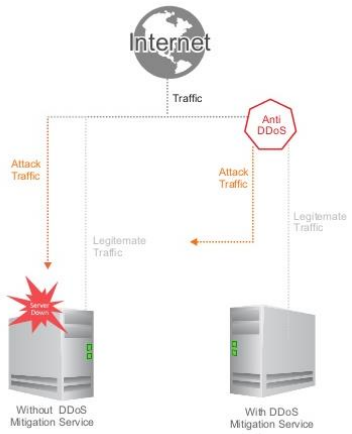

Рис 2. Защита от сетевых атак

Услуги защиты от DDoS-атак предлагают и некоторые поставщики услуг хостинга: анализ сетевого трафика производится в режиме 24/7, поэтому ваш сайт будет в относительной безопасности. Такая защита способна выдержать мощные атаки — до 1500 Гбит/сек. Оплачивается при этом трафик.
Еще один вариант – защита IP-адресов. Провайдер помещает IP-адрес, который клиент выбрал в качестве защищаемого, в специальную сеть-анализатор. При атаке трафик к клиенту сопоставляется с известными шаблонами атак. В результате клиент получает только чистый, отфильтрованный трафик. Таким образом, пользователи сайта могут и не узнать, что на него была предпринята атака. Для организации такого создается распределенная сеть фильтрующих узлов так, чтобы для каждой атаки можно было выбрать наиболее близкий узел и минимизировать задержку в передаче трафика.
Результатом использования сервисов защиты от DDoS-атак будет своевременное обнаружение и предотвращение DDoS-атак, непрерывность функционирования сайта и его постоянная доступность для пользователей, минимизация финансовых потерь от простоев сайта или портала.

2.3 Защита DNS

Обычные файрволы и IPS в защите не помогут, они бессильны против комплексной DDoS-атаки на DNS. На самом деле брандмауэры и системы предотвращения вторжений сами являются уязвимыми для атак DDoS.

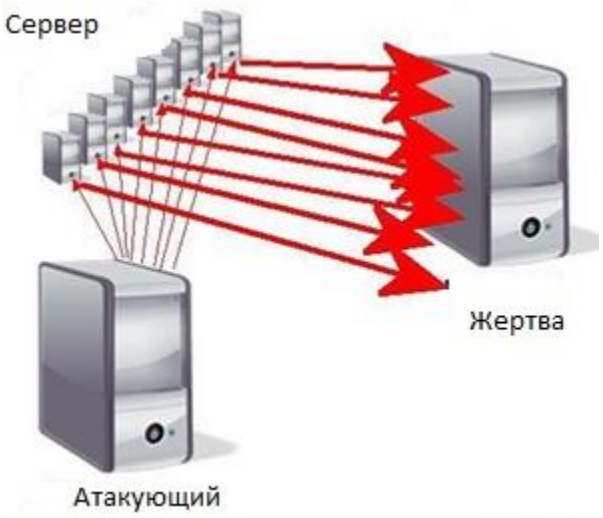

Рис. 3 Защита DNS

На выручку могут прийти облачные сервисы очистки трафика: он направляется в некий центр, где проверяется и перенаправляется обратно по назначению. Эти услуги полезны для TCP-трафика. Те, кто сами управляют своей инфраструктурой DNS, могут для ослабления последствий DDoS-атак принять следующие меры[27].

1. Мониторинг DNS-серверов на предмет подозрительной деятельности является первым шагом в деле защиты инфраструктуры DNS. Коммерческие решения DNS и продукты с открытым исходным кодом, такие как BIND, предоставляют статистику в реальном времени, которую можно использоваться для обнаружения атак DDoS. Мониторинг DDoS-атак может быть ресурсоемкой задачей. Лучше всего создать базовый профиль инфраструктуры при нормальных

условиях функционирования и затем обновлять его время от времени по мере развития инфраструктуры и изменения шаблонов трафика.

2. Дополнительные ресурсы DNS-сервера помогут справиться с мелкомасштабными атаками за счет избыточности инфраструктуры DNS. Ресурсов сервера и сетевых ресурсов должно хватать не обработку большего объема запросов. Конечно, избыточность стоит денег. Вы платите за серверные и сетевые ресурсы, которые обычно не используются в нормальных условиях. И при значительном «запасе» мощности этот подход вряд ли будет эффективным.

3. Включение DNS Response Rate Limiting (RRL) снизит вероятность того, что сервер будет задействован в атаке DDoS Reflection [28]– уменьшится скорость его реакции на повторные запросы. RRL поддерживают многие реализации DNS.

4. Используйте конфигурации высокой доступности. Можно защититься от DDoS-атак путем развертывания службы DNS на сервере высокой доступности (HA). Если в результате атаки «упадет» один физический сервер, DNS-служба может быть восстановлена на резервном сервере.

Лучшим способом защиты DNS от DDoS-атак будет использование географически распределенной сети Anycast. Распределенные сети DNS могут быть реализованы с помощью двух различных подходов: адресации Unicast или Anycast. Первый подход намного проще реализовать, но второй гораздо более устойчив к DDoS-атакам. В случае Unicast каждый из серверов DNS вашей компании получает уникальный IP-адрес. DNS поддерживает таблицу DNS-серверов вашего домена и соответствующих IP-адресов. Когда пользователь вводит URL, для выполнения запроса выбирается один из IP-адресов в случайном порядке. При схеме адресации Anycast разные серверы DNS используют общий IP-адрес. При вводе пользователем URL возвращается коллективный адрес серверов DNS. IP-сеть маршрутизирует запрос на ближайший сервер. Anycast предоставляет фундаментальные преимущества перед Unicast в плане

безопасности. Unicast предоставляет IP-адреса отдельных серверов, поэтому нападавшие могут инициировать целенаправленные атаки на определенные физические серверы и виртуальные машины, и, когда исчерпаны ресурсы этой системы, происходит отказ службы. Anycast может помочь смягчить DDoS-атаки путем распределения запросов между группой серверов. Anycast также полезно использовать для изоляции последствий атаки.

2.4 Обзор механизмов защиты от распределенных атак типа «отказ в обслуживании»

Серьезность проблемы DDOS-атак, их увеличивающаяся частота и продолжительность, изощренность [12, 34] привели к появлению многочисленных защитных механизмов [9, 25–27]. В то же время, хотя и разработаны многие решения, проблема все же остаётся актуальной. Есть несколько серьезных факторов, которые препятствуют исследованиям противодействия DDOS-атакам. Существует множество возможных DDOS атак, очень немногие из которых могут быть обработаны на стороне жертвы. Поэтому необходимо иметь распределенную, возможно, скоординированную систему реагирования. При этом очень важно, чтобы реакция происходила во многих точках Интернета. Поскольку Интернет управляется распределенным образом, широкое развертывание любой защитной системы или сотрудничество между сетями достаточно сложно реализовать. Распределенная система реагирования должна быть развернута сторонами, не подвергающимися прямому ущербу от атаки [14]. Из этого следует необычная экономическая модель; сторона, которая будет поддерживать стоимость развертывания и работоспособности, не является стороной, которая непосредственно извлекает выгоду от системы. Решение этого вопроса, скорее всего, возможно либо законодательным путем, либо внедрение системы защиты должно представлять обоюдный интерес. Для

того, чтобы разработать качественное защитное средство, необходимо иметь хорошее понимание DDOS-атак. Существуют общедоступные анализы популярных инструментов DDOS атак [52, 46], но не хватает информации о частоте различных типов атак (например UDP-наводнение, TCP SYN-наводнение) и параметрах распределенных атак: скорость, продолжительность, размер пакетов, количество атакующих ботов, попытки реагировать и их эффективность, принесенные убытки и т.д. Считается, что публичная отчетность по атакам принесет ущерб деловой репутации, поэтому, как правило, держится в секрете. Рассматривая защитные механизмы от распределенных атак типа «отказ в обслуживании» можно предложить следующую их классификацию, представленную на рисунке 4 [18]: по уровню активности, по степени взаимодействия, по месту развертывания. В классификации по уровню активности выделяют предупреждающие и реагирующие методы защиты. Предупреждающие методы пытаются либо исключить возможность DDOS-атак вообще, либо пытаются выдержать атаку таким образом, чтобы не отказывать в предоставляемой услуге легитимным пользователям [41].

Рисунок 4 –Классификация методов защиты от атак типа «отказ в обслуживании»

Реагирующие методы стремятся смягчить последствия нападения на жертву. Для этого они должны обнаруживать атаки и реагировать на них. В данном случае важно как можно раньше обнаружить атаку и иметь низкую степень ложных срабатываний. Реакция может заключаться в изучении характеристик пакетов и передаче их конкретным реагирующим средствам. В классификации по степени взаимодействия можно выделить три типа: автономные, действующие согласованно (совместно), взаимозависимые. Автономные методы осуществляют независимую защиту в месте, где они развернуты (узел или сеть). В качестве простых примеров автономных методов можно привести межсетевые экраны или системы обнаружения вторжений. Если система выполняет свои функции распределенным образом, она все равно считается автономной, если может полностью развернуться в сети, которую защищает. Совместно действующие методы способны к автономному обнаружению и реагированию, но могут сотрудничать с другими механизмами. При этом производительность в совместной работе часто выше. Взаимозависимые механизмы не могут работать в одной точке развертывания автономно.

Они либо требуют развертывания в нескольких сетях, либо полагаются на другие объекты в задачах предотвращения, обнаружения атак и в эффективном реагировании. Т.е. зависимые механизмы, развернутые на одном маршрутизаторе, не дадут никакой выгоды. От DDOS-атак можно защищаться в разных местах сети, таким образом, защитные механизмы также могут быть классифицированы в зависимости от места развертывания. Елена Мирковик и др. представили три возможных места в Интернете для развертывания DDOS защиты: сеть цели атаки, промежуточные сети, сеть источника атаки [31]. На

рисунке 5 показана упрощенная схема сети Интернет, демонстрирующая различные места для развертывания защитных средств.

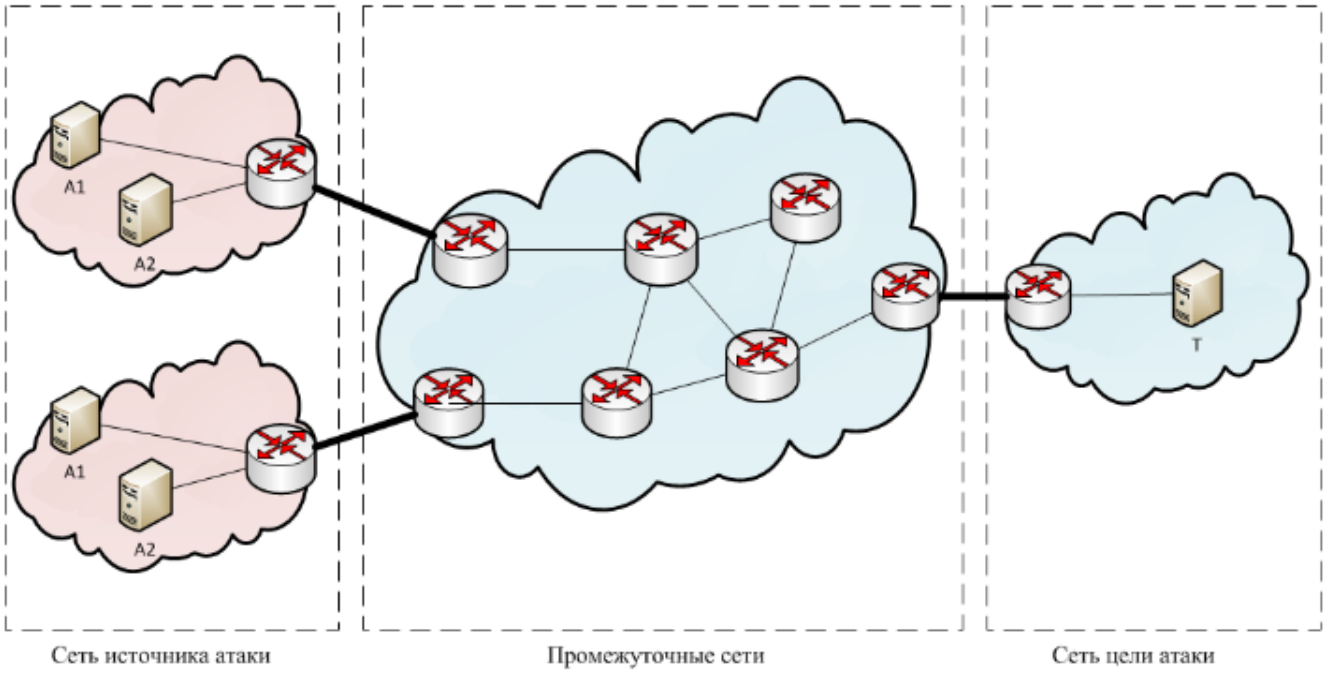

Рисунок 5 – Места развертывания защитных средств

Защитные механизмы также можно рассмотреть с точки зрения их стратегии [41]. Естественно, они будут перекликаться с рассмотренными классификациями, но в отличие от классификаций, стратегии позволяют отразить функциональный аспект защитного средства. Стратегии различных механизмов защиты от DDOS-атак можно разделить на четыре категории представленные на рисунке 5.: предупреждение, выявление, реагирование и толерантность.

Превентивные подходы, как было отмечено, пытаются исключить возможность DDOS-атак или предотвратить атаку до причинения значительного ущерба. Выявление может также быть классифицировано как обнаружение атаки либо идентификация источника атаки. Мониторы обнаружения атаки анализируют события в системе для выявления вредоносных попыток вызвать

отказ в обслуживании. Это важный шаг, прежде чем осуществлять противодействие атаке. Целью идентификация источника атаки является поиск источника атаки независимо от адреса источника, содержащегося в поле вредоносного запроса. Механизмы реагирования, как правило, инициируются после обнаружения атаки, чтобы исключить или свести к минимуму последствия нападения на жертву. Целью стратегии толерантности является минимизация ущерба от атаки, в отсутствие способности дифференцировать вредоносные действия от легитимных действий. Чтобы инициировать механизмы толерантности, необходимо просто знать о том, что система находится под атакой. Основываясь на сходствах различных решений, можно для каждой из четырех категорий защиты выделить несколько типов защитных механизмов. На рисунке 5 показана таксономия защитных механизмов для классификации существующих решений от DDOS атак.

Рисунок 6 – Стратегии механизмов защиты от DDOS-атак

В рамках диссертационного исследования наибольший интерес представляют превентивные механизмы, направленные в большей степени на предотвращение атак и причинения значительного ущерба атакуемым ресурсам. Поэтому в рамках работы мы ограничимся рассмотрением только этой категорией защитных механизмов.

2.5 Превентивные механизмы защиты от DDOS-атак

Превентивные механизмы защиты от DDOS-атак стремятся прекратить атаку до того, как она приведет к повреждению системы. Механизмы предотвращения включают следующие: фильтрация фальсифицированных пакетов, самосертификация адресов, безопасный оверлей.

2.5.1 Фильтрация фальсифицированных пакетов

С целью скрыть происхождение DDOS-атаки многие злоумышленники фальсифицируют IP-адрес. Отраженные атаки и методы усиления атак опираются также на IP-спуфинг. Механизмы фильтрации предназначены для запрещения трафика DDOS-атаки с фальсифицированными адресами источников, путем отброса пакетов с ложными IP-адресами.

Фильтрация недопустимых адресов и валидация адресов источника.

Фильтрация недопустимых адресов и валидация адресов источников определены в требованиях к маршрутизаторам IPv4 IETF RFC 1812[28]. Фильтрация недопустимых адресов указывает маршрутизатору не пересылать все недопустимые пакеты, где недопустимый пакет является пакетом, содержащим в заголовке отправителя или получателя IP-адрес, присвоенный Internet Assigned Numbers Authority(IANA) как IP-адрес специального назначения. Последние IPv4 адреса специального назначения определены в IETF RFC6890[35], другие

примеры недопустимых адресов включают в себя зарезервированное и нераспределенное пространство IP-адресов и адрес назначения 255.255.255.255/32.

Проверка адреса источника указывает, что маршрутизатор должен реализовать возможность фильтрации трафика на основе сравнения адреса отправителя в пакете и таблицы пересылки для логического интерфейса, через который пакет был получен[36]. Если такая фильтрация разрешена, маршрутизатор должен отбрасывать пакет без уведомления, если он был принят через интерфейс, отличающийся от того, через который будет пересылаться пакет, направленный по адресу отправителя. Иными словами, если маршрутизатор не будет пересылать пакет, содержащий данный адрес, через определенный интерфейс, ему не следует доверять этому адресу, указанному в поле отправителя, для пакета, поступившего через тот же интерфейс.

Фильтрация недопустимых адресов исключает возможность подмены для небольшого набора адресов. Злоумышленник может просто изменять подмены любых недопустимых адресов. Проверка адресов отправителя может устранить большинство подмен адресов. Тем не менее, с учетом количества ассиметричных маршрутов в Интернете вполне возможно, что путь возврата к адресу отправителя пакета может не следовать из того же интерфейса, на котором был принят пакет. Таким образом, использование подобной методики фильтрации пакетов может вызвать побочный ущерб для трафика легитимных пользователей.

2.5.2 Входящая/исходящая фильтрация.

Цель входящей/исходящей фильтрации в том, чтобы разрешить входящий или исходящий из сети трафик, только если адреса отправителя находятся в

пределах ожидаемого диапазона IP-адресов. Входная фильтрация относится к фильтрации трафика, входящего в сеть, а выходная фильтрация относится к фильтрации трафика, покидающего сеть. Использование фильтрации на входе в сеть для защиты от DOS- атак описывается в RFC2827 как Best Current Practice(BCP) [34]. Идея входящей/исходящей фильтрации показана на рисунке 6. В соответствии с рисунком первый атакующий находится в сети 198.51.100.0/24, подключение которой к Интернет обеспечивает провайдер A(ISPA). Фильтрация входящего трафика на интерфейсе маршрутизатора R2, который обеспечивает возможность подключения сети атакующего, ограничивает трафик, позволяя принимать лишь те пакеты, где адрес отправителя относится к блоку адресов 198.51.100.0/24 и запрещает злоумышленнику использовать недопустимый адрес отправителя, который не принадлежит другому адресному блоку.

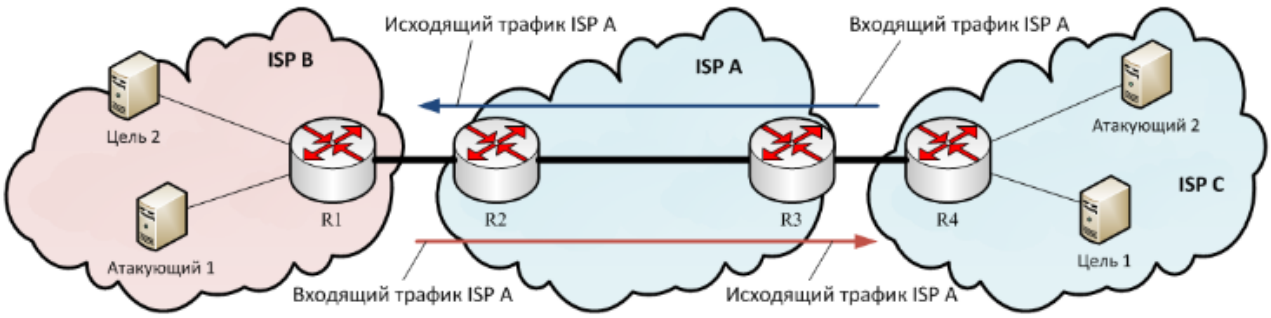

Рисунок 7–Пример входящей/исходящей фильтрации

Фильтр входящих пакетов на маршрутизаторе 2 работает по следующему алгоритму:

 Если адрес отправителя в пакете относится к сети 198.51.100.0/24, то пакет пересылается в направлении получателя.

 Если адрес отправителя в пакете относится к любому другому блоку, то пакет отбрасывается.

Это и есть входящая фильтрация. Если граничный маршрутизатор R1 вместо R2 предоставляет ту же функцию фильтрации, тогда это будет называться исходящей фильтрацией.

Ключевым требованием фильтрации на входе/выходе является знание ожидаемых IP-адресов на определенный порт. В некоторых сетях со сложной топологией не просто получить эту информацию.

2.5.3 Фильтрация на основе маршрута

Парк и Ли предложили распределенную фильтрацию пакетов на основе маршрута (distributed packet filtering, DPF), подходящую для фильтрации потока поддельных пакетов[19]. DPF использует информацию о маршрутизации, чтобы определить, если пакет прибывает на маршрутизатор (например, пограничный маршрутизатор в автономной системе), действующий в отношении зарегистрированных адресов отправителя/получателя, учитывая ограничения доступности налагаемые маршрутизацией и топологией сети. DPF использует информацию топологии маршрутизации BGP для фильтрации трафика с поддельными адресами отправителя.

2.5.4 Защита источника IPv4 (IPv4 Source Guard)

Функция IP Source Guard обеспечивает фильтрацию IPv4-адресов отправителя на интерфейсах второго уровня, чтобы предотвратить вредоносный хост от подмены IP-адреса. IP Source Guard контролирует назначение адресов по протоколу DHCP и использует статические соответствия для автоматической настройки интерфейсов второго уровня для отбрасывания трафика, если IP-адрес

отправителя отличается от IP-адреса, присвоенного этому интерфейсу. Функция IP Source Guard реализуется на коммутаторах, которые используются в маленьких офисах (SOHO) или в сетях на уровне доступа. Данная функция опирается на то, что каждый узел имеет один сетевой интерфейс и каждый сетевой интерфейс имеет один адрес.

Метод «Passport». «Passport»–это метод проверки подлинности адресов отправителя, разработанный Лиу и др.[25]. Он направлен на обеспечение того, что ни хост отправитель, ни АС не могут подменить адресное пространство, что и реализует Passport. На рисунке 6 представлена общая схема работы метода проверки подлинности адресов отправителя.

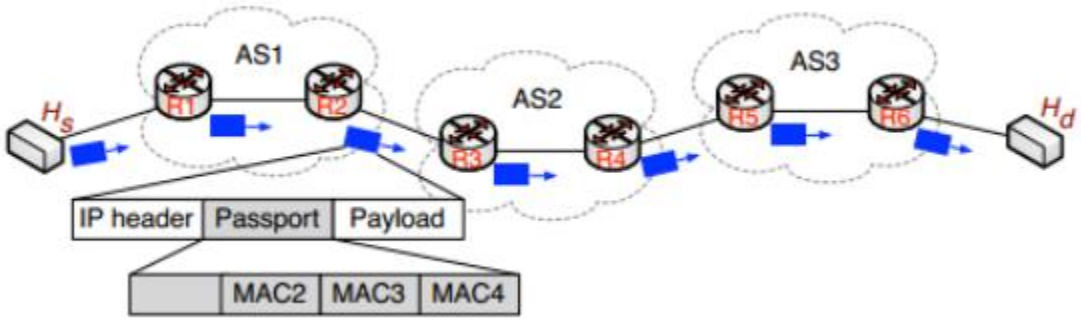

Рисунок 8–Общая схема работы метода проверки подлинности адресов отправителя

Когда пакет покидает свою отправляющую АС, пограничный маршрутизатор отмечает в пакете код аутентификации сообщения (Message Authentication Code, MAC) для каждой АС по пути к сети назначения. Каждый MAC вычисляется с использованием общего для отправляющей АС и следующей по пути АС секретного ключа. Когда пакет входит в следующую по пути АС пограничный маршрутизатор проверяет соответствующий MAC, используя секретный ключ с АС источником. Верификацию маршрутизатор выполняет,

используя адрес отправителя пакета для поиска отправляющей АС, получает общий ключ и пересчитывает MAC. АС может получить соответствие между адресом источника и соответствующей исходящей АС из BGP, используя атрибут пути AS-PATH[30]. Маршрутизатор стирает значение MAC в пакете после верификации, чтобы предотвратить возможность проведения криптоанализа оффлайн. Пакет с неверным MAC в промежуточной АС отбрасывается в АС назначения. Две АС получают парный секретный ключ, который используется для вычисления MAC, путем использования стандартного протокола обмена ключом Диффи-Хеллмана в их BGP анонсах.

Выводы по второй главе

1. Приведена функциональная модель систем защиты и блокирования DDoS атак. Показано, что эффективным средством противодействия атакам может стать только система, аналогичная по сложности исполнения самим атакам. Описана структура и концептуальный алгоритм работы предлагаемой системы.

2. Разработан алгоритм обнаружения управляющего трафика на основе методов интеллектуального анализа данных. Разработанный алгоритм позволяет обнаружить трафик независимо от используемого протокола или организационной структуры ботнета.

3. Предложен метод обнаружения управляющих компонентов атак, с которых осуществляется контроль атаки. Данный метод включает в себя сбор различной информации об адресах предполагаемых злоумышленников, такой, как тип и версия операционной системы, тип устройства, запущенные службы, порты, маршрут следования данных, DNS информация, регистрационные данные whois, географическое местоположение узла, уязвимости узла. Данная информация может иметь важное значение в процессе расследования инцидента.

ГЛАВА 3 МЕТОДИКА ЗАЩИТЫ ОТ DDOS АТАК

3.1 Программная система выявления DDoS атак

DDoS нападение распознать просто – замедление работы сети и серверов, заметное как администратору системы, так и обычному пользователю. Первым шагом в защите должны идентифицировать тип трафика, который загружает рассматриваемую сеть. Большинство нападений DDoS посылает очень определенный тип трафика - ICMP, UDP, TCP, часто с поддельными IP адресами. Нападение обычно характеризует необычно большое количество пакетов некоторого типа. Исключением к этому правилу являются DDoS нападения, направленные против определенных служб, типа HTTP, используя допустимый трафик и запросы.

Чтобы идентифицирвать и изучить пакеты, мы должны анализировать сетевой трафик. Это можно сделать двумя различными методами в зависимости от того, где исследуется трафик. Первый метод может использоваться на машине, которая расположена в атакуемой сети. Tcpdump - популярный сниффер, который хорошо подойдет для наших целей. Анализ трафика в реальном масштабе времени невозможен на перегруженной сети, так что мы будем использовать опцию "-w", чтобы записать данные в файл. Затем, используя инструмент типа tcpdstat или tcptrace, мы проанализируем результаты. Результаты работы tcpdstat, на нашем tcpdump файле:

DumpFile: test

FileSize: 0.01MB

Id: 200212270001

StartTime: Apr Tue 1 00:01:51 2014

EndTime: Apr Tue 1 00:02:15 2014

TotalTime: 23.52 seconds

TotalCapSize: 0.01MB CapLen: 96 bytes

# of packets: 147 (12.47KB)

AvgRate: 5.56Kbps stddev:5.40K   PeakRate: 25.67Kbps

IP flow (unique src/dst pair) Information

of flows: 9 (avg. 16.33 pkts/flow)

Top 10 big flow size (bytes/total in %):

 26.6% 16.5% 14.7% 11.6% 9.8% 7.6% 5.4% 5.4% 2.5%

IP address Information

of IPv4 addresses: 7

Top 10 bandwidth usage (bytes/total in %):

 97.5% 34.1% 31.2% 21.4% 10.7% 2.5% 2.5%

Packet Size Distribution (including MAC headers)

<<<<

[32-   63]:   79

[64- 127]:   53

[128- 255]:   8

[256- 511]:   6

[512- 1023]:   1

>>>>

Protocol Breakdown

<<<<

protocol	packets	bytes	bytes/pkt
[0] total	147 (100.00%)	12769 (100.00%)	86.86
[1] ip	147 (100.00%)	12769 (100.00%)	86.86
[2] tcp	107 (72.79%)	6724 (52.66%)	62.84
[3] telnet	66 (44.90%)	3988 (31.23%)	60.42
[3] pop3	41 (27.89%)	2736 (21.43%)	66.73
[2] udp	26 (17.69%)	4673 (36.60%)	179.73
[3] dns	24 (16.33%)	4360 (34.15%)	181.67

[3] other 2 (1.36%) 313 (2.45%) 156.50
[2] icmp 14 (9.52%) 1372 (10.74%) 98.00

Эти простые утилиты могут быстро помочь определить тип преобладающего трафика в сети. Они позволяют сэкономить много времени, анализируя и обрабатывая зафиксированные пакеты.

Для контроля входящего трафика может использоваться маршрутизатор. С помощью списков ограничения доступа, маршрутизатор может служить основным пакетным фильтром. Скорее всего он также служит шлюзом между вашей сетью и интернетом. Следующий пример от Cisco иллюстрирует очень простой способ использовать списки доступа, чтобы контролировать входящий трафик:

access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any
interface serial 0
ip access-group 169 in

Используя команду "show access-list", система покажет количество совпавших пакетов для каждого типа трафика:

Extended IP access list 169
permit icmp any any echo (2 matches)
permit icmp any any echo-reply (21374 matches)
permit udp any any eq echo
permit udp any eq echo any

permit tcp any any established (150 matches)

permit tcp any any (15 matches)

permit ip any any (45 matches)

Результаты просты, но эффективны – обратите внимание на высокое число ICMP echo-reply пакетов. Подробная информация может быть собрана о подозреваемых пакетах, добавляя в конец команду "log-input" к специфическому правилу. Это правило будет регистрировать информацию о любом ICMP трафике:

access-list 169 permit icmp any any echo-reply log-input

Маршрутизатор теперь более подробно регистрирует собранные данные (которые можно посмотреть используя "show log") о соответствующих пакетах. В пример ниже, файл регистрации показывает несколько пакетов, соответствующих правилу DENY ICMP:

%SEC-6-IPACCESSLOGDP:list 169 denied icmp 192.168.45.142 (Serial0 *HDLC*) ->10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113 (Serial0 *HDLC*)->10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.72 (Serial0 *HDLC*)->10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.154 (Serial0 *HDLC*)->10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.15 (Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142 (Serial0 *HDLC*) -> 0.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.47 (Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.35 (Serial0 *HDLC*) -> 0.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113 (Serial0 *HDLC*) -> 0.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.59 (Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.82 (Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.56 (Serial0 *HDLC*)->10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.84 (Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.47 (Serial0 *HDLC*)->10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.35 (Serial0 *HDLC*) ->10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.15 (Serial0 *HDLC*)->10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.33 (Serial0 *HDLC*) ->10.2.3.7 (0/0), 1 packet

Обратите внимание на информацию, содержавшуюся в каждой строке: источник и адрес назначения, интерфейс и правило, которому оно соответствует. Этот тип детальной информации поможет определить нашу защиту.

Реакция

После того, как мы идентифицировали подозреваемый трафик, пришло время исследовать, как нам ответить на нападение. К сожалению, варианты несколько ограничены, потому что большинство DDoS нападений использует поддельные

исходные IP адреса, которые вероятно сгенерированы случайным образом.

Отслеживаем источник атаки

Первое, что приходится делать, это попытаться отслеживать источник атаки. Однако DDoS, в отличие от традиционного DoS, исходит из множественных источников. Поэтому неплохо было бы определить транзитный маршрутизатор, через который проходят большинство пакетов. К сожалению, для этого потребуется сотрудничать с несколькими источниками, так как вы не способны исследовать пакеты на вышестоящих маршрутизаторах. Каждый участник процесса (главным образом ISP провайдеры) будут использовать очень похожие методы. Идентифицировав злонамеренный тип трафика, используя вышеописанные методы, будет создан новый список ограничения доступа. Добавив его к правилам, которые применены к интерфейсу, который посылает трафик атакуемому адресату, мы снова используем команду "log-input". Регистрация подробно запишет информацию об исходном интерфейсе и MAC адресе источника атаки. Эти данные могут использоваться, чтобы определить IP адрес маршрутизатора, отправляющего злонамеренный трафик. Процесс будет повторен на следующем маршрутизаторе в цепочке. После нескольких итераций, источник (или один из них) будет обнаружен. Тогда можно создать соответствующий фильтр, который заблокирует атакующего. Недостаток в этом методе защиты от DDoS нападения – время и сложность. Получение таких данных требует работы с несколькими сторонами, и иногда использование правового принуждения.

Ограничение допустимого предела (“rate limit”)

Лучший способ немедленной помощи, доступный большинству ISP провайдеров, должно быть “ограничение допустимого предела” злонамеренного типа трафика. Ограничение допустимого предела ограничивает пропускную способность, которую определенный тип трафика может потреблять в данный момент времени.

Это может быть достигнуто, удаляя полученные пакеты, когда превышен некоторый порог. Полезно, когда определенный пакет используется в нападении. Cisco предлагает способ, который позволяет ограничить ICMP пакеты, используемые в нападении:

interface xy rate-limit output access-group 2020 3000000 512000 786000 conform-action transmit exceed-action drop access-list 2020 permit icmp any any echo-reply

Этот пример поднимает интересную проблему, которая была отмечена ранее. Что, если злонамеренный трафик полностью законный? Например, ограничение SYN flood, направленное на Web сервер, отклонит и хороший и плохой трафик, так как все законные подключения требуют начального установления связи. Это трудная проблема, не имеющая простого ответа. Нельзя просто защитится от таких типов хитрых DDoS нападений, не принося в жертву часть законного трафика.

Фильтрация черной дыры

ISP провайдеры могут использовать другие способы защиты, которые зависят от изменения маршрутизации, типа фильтрации “черных дыр”. “Black hole” фильтрация отправляет злонамеренный трафик к воображаемому интерфейсу, известному как Null0 – подобный /dev/null на Unix машинах. Так как Null0 - не существующий интерфейс, трафик, направленный к Null0, по существу удаляется. Кроме того, эта методика минимизирует воздействие производительности, так как остальная часть сети остается устойчивой при тяжелых загрузках.

Важно отметить, что адресная фильтрация - не лучший способ защиты против DDoS нападений. Даже если вы заблокировали нападение на своем маршрутизаторе или межсетевой защите – все еще большие порции входящего трафика могут затруднить прохождение законного трафика. Чтобы действительно облегчить эффект от DDoS нападения, трафик должен быть блокирован в вышестоящей цепочке – вероятно на устройстве, управляемом большим провайдером. Это означает, что многие из программ, которые утверждают, что

предотвращают DDoS нападения, в конечном счете, бесполезны для маленьких сетей и их конечных пользователей. Кроме того, это означает, что предотвращение DDoS нападения, в некоторый момент, не зависит от нас. Это печальная правда, понятная любому, кто когда-либо имел дело с проблемой.

3.2 Предотвращение от атак

Блокировка нежелательных запросов через htaccess. Работа с файлом .htaccess дает возможность на уровне сервера управлять доступом к сайту, не затрагивая коды и скрипты, за счет чего он нагружает ресурс очень слабо. При этом защита сайта осуществляется при помощи введений ограничений по IP-адресам и определенным признакам в запросах.

Защита с помощью PHP-скрипта. Каждый поступивший на сайт запрос анализируется, а IP, от которого он исходил, запоминается. Если команды поступают с привычного IP в промежутки, нетипичные для человека, то ему блокируется доступ к странице. К недостатку данного способа можно отнести то, что от работы скрипта нагрузка на сайт может повыситься.

Сервис для очистки от спамного трафика. К доменному имени вашего сайта добавляется DNS-сервер компании, которая предоставляет услуги защиты. В результате все запросы, поступающие на ваш сайт, сначала идут на IP-адрес фильтрующего сервера. Безопасные пакеты направляются на хостинг вашего ресурса, а подозрительные блокируются. В результате всю лишнюю нагрузку берет на себя специальный сервер.

Необходимо включить команду "ip verify unicast reverse-path" (или не Cisco эквивалент) на входном интерфейсе подключения восходящего потока данных. Эта особенность удаляет поддельные пакеты, главную трудность в защите от DDoS нападений, прежде, чем они будут отправлены. Дополнительно, удостоверьтесь, что блокирован входящий трафик с исходными адресами из

зарезервированных диапазонов (то есть, 192.168.0.0). Этот фильтр удалит пакеты, источники которых очевидно неправильны.

Входящие и исходящие методы фильтрации, также критичны для предотвращения DDoS нападений. Эти простые списки ограничения доступа, если внедрены всеми ISP провайдерами и большими сетями, могли бы устранить пересылку поддельных пакетов в общедоступный интернет, сокращая тем самым время, требуемое для розыска атакующего. Фильтры, помещенные в граничные маршрутизаторы, гарантируют, что входящий трафик не имеет исходного адреса, происходящего из частной сети и что еще более важно, что трафик на пересекающихся курсах имеет адрес, происходящий из внутренней сети

Рис 7. Схема защиты от DDoS атак методом PHP скрипта

3.3 Разработанная методика защиты от DDoS атак

Методы защиты от распределенных атак отказа в обслуживании можно разделить на две группы: это методы, предшествующие совершению атаки,

направленные на предотвращение атаки и методы, применяющиеся впоследствии начала атаки, это методы противодействия и смягчения результатов атаки.

К первому методу можно отнести организационно-правовые мероприятия. К примеру, недопустимость вовлечения в конфликтные ситуации, или меры, направленные на ликвидацию результатов, которых хочет добиться злоумышленник, разграничение и маскировка критичных ресурсов.

Когда уже началась атака, используются активные меры, направленные на противодействия атакам. Основными из этих мер являются увеличение ресурсов и фильтрация трафика.

Существуют методы и средства, организующие защиту непосредственно внутри атакуемой сети. Их выделяют в подгруппу средств, расположенных не на границе сети, а на атакуемой стороне. Среди таких систем можно выделить две группы программных средств:

- средства, которые действуют на уровне операционной системы сервера, на которую направлена атака;
- средства, которые действуют на уровне приложения.

К первой группе средств относят программные файэрволлы и специализированные средства. К примеру, Conlimit - позволяет настроить определенные ограничения для подключений. DDoS deflate – аналог Conlimit, в случае превышения установленных ограничений, блокирует доступ на некоторое время.

Ко второй группе средств можно отнести различные плагины и дополнительные модули для баз данных, веб-серверов, почтовых серверов и других сетевых сервисов.

К примеру, mod_evasive для веб-сервера Apache блокирует на основании различных правил: ограничение по количеству запросов, адресу и т.д.

Однако, вышеприведенные средства осуществляют только блокировку в соответствии с набором указанных правил и не проводят полноценный анализ трафика. То есть они явно недостаточны для противодействия распределенным сетевым атакам. Основным критерием для блокирования трафика является превышение заданного количества запросов с одного адреса. Но данное решение является не корректным определением вредоносного трафика, потому что под него могут попасть различные частные случаи превышения установленных ограничении и запросы из различных сетей, находящихся за прокси-сервером.

При этом потребность в средствах обнаружения и противодействия, реализованных на стороне сервера, существует. Об этом свидетельствуют различные самостоятельные решения системных администраторов, которые появляются в Интернете. Эти решения основаны на проведении некоторого анализа сходящего трафика, и обычно поверхностно, и по результатам этого анализа частично блокировать вредоносный трафик.

При этом анализ вредоносного трафика на уровне атакуемого сервера или приложения имеет большие возможности, так как появляются данные для выявления злоумышленника.

Представляемое решение является централизованным методом защиты от распределенных атак типа DDoS. Для анализа трафика используются log-файлы.

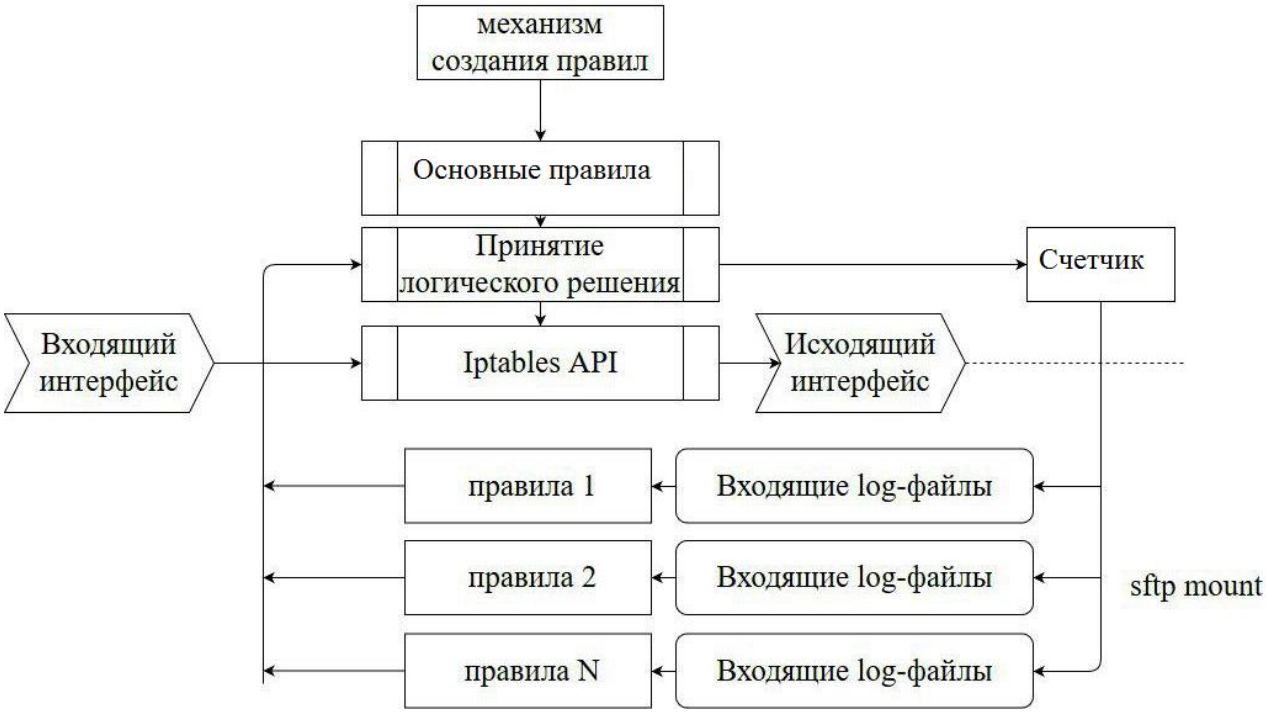

Рис.9 Логика работы алгоритма защиты от DDoS атак

Функциональные возможности разрабатываемой программной системы позволят:

1. Проводить поиск зараженных файлов, загруженных с веб-ресурса;
2. Контролировать действия IP адресов;
3. Блокировать и направлять в null - адрес трафик, помеченный как вредоносный;
4. Проверять загруженные файлы на наличие вирусов с помощью антивируса Clawm;
5. Анализировать и проводить мониторинг серверов с использованием метода передачи log-файлов на сервер фильтрации, в режиме реального времени;
6. Извлекать с заданным интервалом времени актуальные данные из файла access.log.

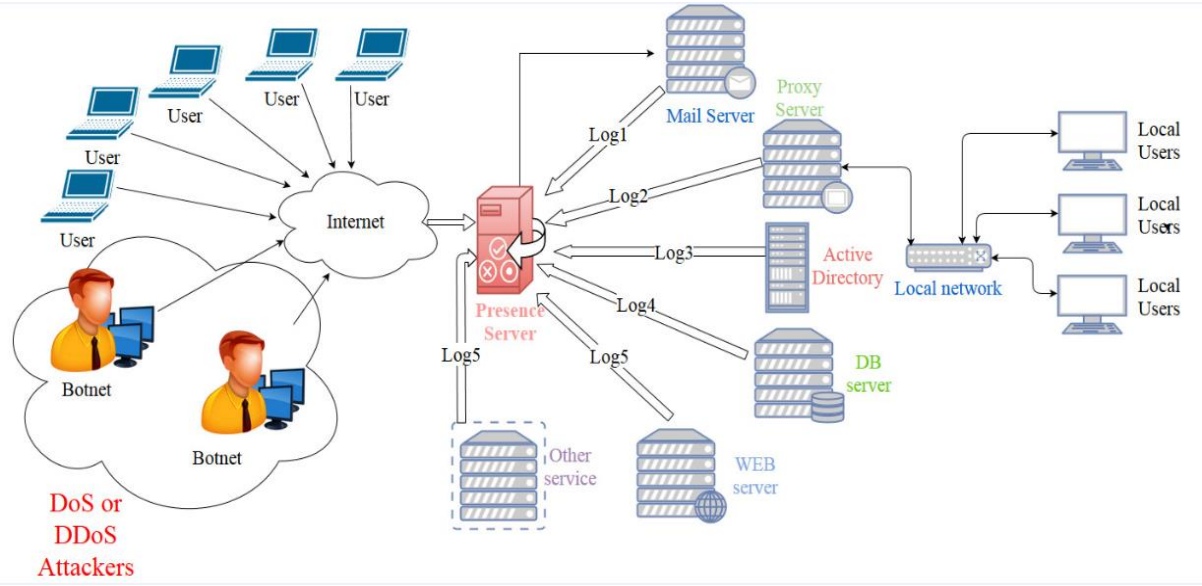

Рис. 10 Схема работы разработанной программной системы

На сервер фильтрации будут подключены сервера различной функциональности (почтовый сервер, сервер базы данных, прокси-сервер, веб-сервер). С помощью программной системы, установленной на сервере фильтрации будет контролироваться работа подключенных серверов в режиме реального времени. Сервер фильтрации будет контролировать наличие подозрительных запросов, и в случае обнаружения будет их блокировать со следующего раза и направлять в null - адрес. Программное обеспечение написано на таких языках высокого уровня, как C/C++ и работает в операционных системах Linux.

В DDOS-атаке в роли атакующего выступает так называемая бот-сеть, или зомби-сеть. Зомби- сеть может насчитывать от нескольких десятков до тысяч хостов. Обычно это нейтральные компьютеры, которые в силу каких-то причин (отсутствие файрвола, устаревшие базы антивируса и т.д.), были заражены, вредоносными программами. Программы, работая в фоновом режиме, непрерывно посылают запросы на атакуемый сервер, выводя его таким образом из строя [21].

В настоящий момент не существует какого-то универсального средства для противодействия DDOS-атакам. Даже такие крупные компании, как Microsoft, eBay, Amazon, Yahoo, страдают от DDOS-атак и не всегда могут с ними справиться [22].

Для противодействия распределенным атакам, направленным на отказ в обслуживании, требуется выполнение двух основных задач [23].

1. Диагностировать DDOS-атаку на самых ранних стадиях. Чем раньше будет обнаружена DDOS-атака, тем раньше сможет включиться в игру сетевой администратор и тем раньше можно будет начать проводить антиDDOS-мероприятия. Кроме того, при обнаружении DDOS-атаки можно будет, не дожидаясь реагирования администратора, автоматически запустить мероприятия по противодействию: задействовать резервные каналы связи, включить фильтры и т.д.
2. Вторая задача связана с разделением общего потока трафика на вредоносный и обычный. Поняв, какие из клиентских запросов являются результатом DDOS-атаки, можно будет создать соответствующие правила для межсетевого экрана или ACL правила для маршрутизатора или же, в случае масштабной атаки, передать эти данные на вышестоящие маршрутизаторы.

Первая из этих задач является достаточно новой. Несколько лет назад основной являлась именно задача по «сортировке» трафика. Однако злоумышленники постоянно совершенствуют способы проведения атак такого типа. И современные атаки отличаются сложностью и наличием этапа подготовки. Во время подготовительного этапа злоумышленник пытается выявить наиболее уязвимые для атаки места. Например, для web-сервера такими местами могут быть определенные скрипты, которые совершают большое количество запросов к базе данных или чрезмерно используют процессорное время. Для выявления этих мест злоумышленник может

совершать серию мини-DDOS- атак на различные скрипты, отслеживая при этом время ответа сервера и время выполнения скрипта. Найдя уязвимое место, злоумышленник сможет парализовать работу сервера, используя бот-сеть меньшего размера. С другой стороны, если диагностировать атаку удастся уже на этом этапе, можно будет задействовать автоматические средства предотвращения атаки, а у системного администратора будет время подготовиться – оптимизировать скрипты, чрезмерно загружающие ресурсы компьютера, создать фильтры и т.д.

Для обнаружения DDOS-атак и создания специальных фильтров для отсечения вредоносного трафика применяются разнообразные методы и подходы.

Среди основных методов можно выделить методы, базирующиеся на статистическом анализе. Это количественный анализ, анализ среднеквадратичных отклонений, кластерный анализ и т.д. Все эти виды анализа могут оценивать различные параметры сетевой активности и диагностировать начало атаки либо определять вредоносный трафик.

Основными параметрами, по которым проводится анализ, могут быть:

- Количество запросов за определенный период.
- Скорость поступления запросов.
- Количество запросов с определенного источника или из определенной сети.
- Количество запросов к определенному пункту назначения (для web-сервера это конкретный скрипт).
- Время между запросами.
- Другие различные параметры сетевой активности.

С помощью среднеквадратичного отклонения можно рассчитать допустимую границу для одного из параметров сетевой активности, например, для количества запросов за какой-то период времени. В случае если граница будет нарушена, это станет свидетельством начала атаки. Так как в разное время нагрузка на сетевой

ресурс, так же может быть разной, то для раннего обнаружения атаки необходим постоянный мониторинг и пересчет границ для каждого временного шага. Постоянный мониторинг позволит определить атаку, если она начнется в период небольшой сетевой активности, или, если злоумышленник ищет потенциально уязвимые места на сервере, проводя мини-DDOS- атаки и изучая поведения сервера. В случае если верхняя граница задана строго и злоумышленник проводит мини-атаки в период наименьшей сетевой активности, он может не нарушать заданную границу, и его действия будут не обнаружены. Атака будет обнаружена тогда, когда злоумышленник найдет потенциально уязвимое место, и предпримет на него атаку. Постоянный мониторинг активности и перерасчет допустимых границ позволяет этого избежать. В период меньшей сетевой активности верхняя граница снизится. Однако и этот метод имеет ряд минусов.

Во-первых, злоумышленник может начать атаку постепенно. Показатели активности на каждом шаге будут плавно повышаться, но при этом не будут нарушать границ. Так как при расчете средне-квадратичного отклонения используются последние n интервалов, в том числе и те, которые уже содержат данные атаки, то злоумышленник, постепенно увеличивая интенсивность атаки, будет отодвигать границу.

Во-вторых, выбор размера периода n для расчета среднеквадратичного отклонения, не является однозначным.

Если n будет слишком велико, полученная граница будет слишком высоко, если используется малое значение n, то возможны частые срабатывания. Выбрать же оптимально значение n в этой ситуации будет невозможно, так как любое его значение может захватывать два разных периода. Например, даже малое значение n, рассчитываемое в начале рабочего дня, будет захватывать данные и ночного периода, связанного с низкой активностью, и дневного периода, который характеризуется большей нагрузкой на сетевые ресурсы.

Для того чтобы предотвратить ложное срабатывание, связанное с началом рабочего дня, потребуется использовать такое значение n, в котором будут данные за несколько дней. Либо контролировать сразу несколько временных периодов – при срабатывании на минутных интервалах, рассмотреть часовые или суточные периоды. Но это в свою очередь приведет к уменьшению точности, и атака будет определена с опозданием [54].

В качестве гипотезы можно предположить, что более высокую точность в этих случаях может дать учет различных периодов активности и сравнение сходных между собой периодов.

Пусть xi количество запросов к серверу за один час. Сервер испытывает стабильную суточную нагрузку. Количество суточных периодов n. Тогда запросы к серверу можно записать в виде матрицы:

$$x1\ 1, x1\ 2\ , x1\ 3\ \ldots x1\ \ 24\ ,$$
$$x2\ 1, x2\ 2\ , x2\ 3\ \ldots x2\ \ 24\ ,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$xn\ 1, xn\ 2\ , xn\ 3\ \ldots xn\ 24.$$

Каждая строка матрицы включает в себя суточные данные о количестве запросов. Первая строка отражает данные текущих суток, в этой связи она может быть заполнена не до конца. Расчет среднеквадратичного отклонения в этом случае может проводиться двумя способами [35]:

- Обычным способом с учетом определенного числа последних значений, например так:

$$x2\ 1, x2\ 2\ , x2\ 3\ \ldots x2\ 24, x1\ 1, x1\ 2\ , x1\ 3\ , x1\ 4.$$

Значения берутся из строк матрицы.

•С учетом сезонности. Расчет проводится по столбцам:

xn 1, … x2 1, x1 1.

Если мы находимся в i-м периоде, можно рассчитать границу для (i + 1)-го периода, используя значение (i + 1)-го столбца. Если сетевой ресурс испытывает нагрузку, связанную с недельными или суточными циклами, то необходимо исключить строки, которые соответствуют праздничным и выходным дням. Или даже использовать только каждую седьмую строку, т.е. сравнивать, например, только период с 11:00 до 12:00, для каждого понедельника.

Проверка гипотезы

Апробация данной гипотезы проведена на реальных данных, полученных из лог-файлов различных web-сайтов, которые содержат в себе нормальные данные и данные, соответствующие DDOS-атакам.

Список рассматриваемых сайтов:

https://tuit.uz

http://dcs.tuit.uz

http://acm.tuit.uz

Лог-файл представляет собой стандартный файл access_log web-сервера Apache.

Предварительно данные из лог-файлов были обработаны вручную и проанализированы. В результате были выделены сезонные периоды, а также точно обозначено время начала атак.

Диагностирование DDOS-атаки проводилось различными методами:

- Анализ сходных сезонных периодов.
- Анализ последних n периодов, при различных значениях n.
- Анализ последних n периодов, различной размерности (минуты, часы и т.д.), для разных значений n.

В связи с тем, что лог-файлы имеют свой специфичный формат, их анализ стандартными методами является затруднительным. Для проведения анализа был

создан скрипт, извлекающий из лог- файла необходимые данные и экспортирующий их в базу данных. Скрипт был реализован с помощью языка fail2ban . Предпочтение данному языку программирования отдано в связи с наличием богатого инструментария по работе со строками и регулярными выражениями [46]. В качестве системы управления базами данных выбрана свободно распространяемая СУБД MySQL версии 5.5.23. Использование СУБД позволило ускорить процесс обработки и анализа данных и сделать его более гибким.

Для проведения собственно самого анализа также была разработана отдельная программа. Язык реализации программы C/C++ python . Его использование позволило выдержать созданный программный комплекс в одном ключе и дало возможность реализовать CLI-интерфейс. CLI-интерфейс может быть доступен для системного администратора с любого компьютера, что позволяет в удаленном режиме диагностировать атаку и выявлять во входящем трафике различные аномалии. В дальнейшем планируется доработать программу для работы в полностью автоматическом режиме. В этом случае данные из лог-файла будут экспортироваться в базу данных в режиме реального времени. Анализ должен происходить после каждого нового добавления данных. В случае диагностирования начала атаки программа будет рассылать необходимые уведомления и автоматически задействовать мероприятия по противодействию атаке.

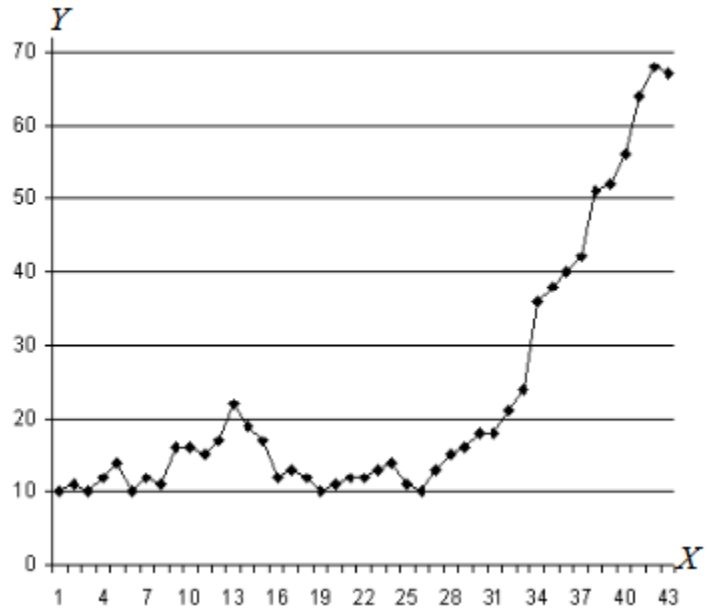

Рис. 11. Количество запросов в период начала DDOS-атаки, 10-минутный интервал

Метод анализа с учетом сезонности показал более высокую точность обнаружения DDOS- атаки и более короткое время, которое прошло с момента начала атаки до её диагностирования.

На графике отражается количество запросов к серверу за секунду, соответствующие периоду начала DDOS-атаки. Ось X – временной интервал. Одно деление соответствует 10 мин. Ось Y – количеству запросов к серверу за секунду.

На основании IP-адресов, принадлежащих компьютерам бот-сети, которые были выявлены при анализе лог-файлов, удалось точно установить момент начала атаки. На графике он соответствует 24-му периоду. Учет сезонности помог выявить DDOS-атаку уже в 31-м периоде. Другие методы показали худшие результаты. При слишком больших значениях n атаку удалось диагностировать только на 42-м периоде, при малых происходило ложно срабатывание в 14-м периоде.

В среднем по всем тестам время обнаружения DDOS-атаки методами с учетом сезонности, сократилось в 4 раза, так же сократилось число ложных срабатываний.

Достаточно большой сложностью, возникающей при использовании данного метода, является правильный выбор сходных между собой периодов. Для апробации были выбраны данные с таких серверов, периоды работы которых однозначно определялись и не вызывали сомнения. Однако определить различные периоды в работе, например, крупного магистрального маршрутизатора, достаточно сложно. Его активность может не подчиняться суточным или недельным периодам, но также иметь свои периоды, которые могут представлять собой сложные периоды, получаемые в результате сложения активностей различных групп пользователей, например пользователей из разных часовых поясов. Кроме того, уже существующие сезонные периоды могут изменяться, к ним могут добавляться новые периоды, поэтому при постоянном мониторинге трафика необходимо будет проводить его кластеризацию и выявлять новые сезонные периоды в работе.

ЗАКЛЮЧЕНИЕ

В данной работе предложена методика раннего обнаружения начала DDoS-атаки и последующего определения вредоносных запросов. В основе разработанных методик лежат методы теории вероятности, кластерного и статистического анализа, принципы машинного обучения. В качестве основных результатов диссертационной работы можно выделить следующие:

1.Проведен мониторинг современных распределенных атак, направленных на отказ в обслуживании. Выделена новая группа атак средней и малой интенсивности, направленных в основном на региональные ресурсы. Проведен мониторинг различных программных и аппаратных средств противодействия и средств обнаружения атак такого типа. Выявлено отсутствие средств, позволяющих адекватно решать поставленные задачи по обнаружению и противодействию, для данной группы атак.

2.Предложена и обоснована гипотеза о существовании сезонности в работе различных сетевых ресурсов. Выяснены причины, влияющие на формирования и особенности сезонных периодов.

3.Предложено формальное описание сезонности сетевой нагрузки, которое позволяет выявлять сезоны различной периодичности, отличающиеся учетом неопределенного начала и завершения периода.

4. Исследование модели атаки позволило создать методику раннего обнаружения и противодействия DDoS-атакам средней и малой интенсивности. Методика является универсальной, учитывает, как региональные особенности, так и другие факторы, и может быть применена для обнаружения и противодействия DDoS-атакам различных типов и различной мощности. А также для обнаружения аномальных данных в различных сферах деятельности..В

процессе разработки методики создано два алгоритма: алгоритм определения точки начала атаки и алгоритм разделения смешанного трафика на благонадежный и вредоносный. Отличительной чертой алгоритмов является учет сезонных колебаний сетевой нагрузки.

6. Для алгоритма по разделению трафика выработаны критерии успешности. Данные критерии являются универсальными и позволяют не только оценить успешность работы алгоритма, но и других, сторонних средств по фильтрации трафика.

7. На основе предложенной методики разработано программное средство по обнаружению начала атаки и последующего обнаружения и блокировки вредоносных запросов. Разработанное средство отвечает требованиям кроссплатформенности, универсальности, открытости. Отличительной чертой разработанного средства является модульность и универсальность. При незначительном изменении отдельных модулей средство может быть применено для обеспечения безопасности различных сетевых ресурсов и их защиты от атак различных типов.

Для апробации результатов диссертационной работы и проведению экспериментов по изучению распределенных атак, направленных на отказ в обслуживании, на базе реальных компьютеров была создана крупная, специализированная нагрузочная сеть. В рамках сети возможно проведение нагрузочных тестов, эмулирующих DDoS-атаки. Нагрузочная сеть поддерживает создание сценариев и проведение упрощенных DDoS-атак на основе данных о реальных атаках. В этом случае проводимые атаки, по сути, являются уменьшенными копиями реальных атак. Проводимые нагрузочные тесты отвечают основным требованиям эксперимента. Возможно повторение теста, необходимое количество раз, фиксация его результатов.

По результатам проводимых в нагрузочной сети тестов, также разработана методика по выявлению уязвимых DDoS-атакам скриптов и модулей в системах управления содержанием и последующей оптимизации. Результаты диссертационной работы соответствуют целям и задачам, поставленным во введении.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Закон Республики Узбекистан «О принципах и гарантиях свободы информации», http://www.lex.uz/acts/82956
2. Концепция информационной безопасности, http://uza.uz/ru/society/v-uzbekistane-razrabatyvaetsya-kontseptsiya-informatsionnoy--31-01-2018
3. DDOS-атаки [Электронный ресурс]. – Режим доступа: http://localname.ru/soft/ataki-tipa-otkaz-v-obsluzhivanii-dos-i-raspredelennyiy-otkaz-v-obsluzhivanii-ddos.html, свободный (дата обращения: 24.04.2012).
4. Соколов А.В. DDoS-атаки как форма политической активности // Соколов А.В., Кирилова Е.В. // Политический процесс в региональном измерении: история, теория, практика. – 2013. – С. 122–125.
5. Афанасьев А. DDOS: противостояние. Как происходят атаки и как их отражать // Системный администратор. Синдикат 13. М. –2010. No1. –2 (122-123). – С. 59–61
6. Бенкен Е.С. PHP, MySQL, XML. Программирование для Интернета [Текст] СПб.: БХВ-Петербург, 2011.
7. Вопросы обеспечения защиты информационных систем от ботнет атак https://cyberleninka.ru/article/v/voprosy-obespecheniya-zaschity-informatsionnyh-sistem-ot-botnet-atak, 2016.
8. Предотвращение атак с распределенным отказом в обслуживании (DDoS) Официальный сайт компании Cisco [Электронный ресурс]. – Режим доступа: http://www.cisco.com/web/RU/products/ps5887/products_white_paper0900aecd8011e927_.html, свободный (дата обращения: 24.04.2012).
9. Методы защиты от DDOS нападений [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/analytics/216251.php, свободный (дата обращения: 24.04.2012).
10. Терновой О.С. Раннее обнаружение DDOS- атак методами статистического анализа/ Перспективы развития информационных технологий. – Новосибирск: Сибпринт, 2012. – С. 201–212. 5.БоровковvА.А. Математическая статистика. Оценка параметров проверки гипотез. – М.: Наука. 1984. – 280 с
11. Бенке Е.С. PHP, MySQL, XML. Программирование для Интернета. – СПб.: БХВ-Петербург, 2011. – С. 336.
12. Дистрибутивы GNU/Linux, основанные на Debian [Электронный ресурс] / URL: http://www.debian.org/misc/children-distros

13. Log files [Электронный ресурс] / URL: http://httpd.apache.org/docs/2.2/logs.html
14. Singh S., Silakari S. An ensemble approach for feature selection of Cyber Attack Dataset // International Journal of Computer Science and Information Security.2012.-Vol. 6, No 2. -P. 297-302.
15. Родионов А.С. Анализ средств противодействия одному виду атак типа «отказ в обслуживании» // Родионов А.С., Шахов В.В. // «Вестник Новосибирского государственного университета. Серия: Информационные технологии». 2008. Т. 6. No2. –С. 80–87.
16. Статистика сайта amic.ru [Электронный ресурс] / URL: http://www.liveinternet.ru/stat/amicru/
17. Методы кластерного анализа. Итеративные методы. [Электронныйресурс] /URL:http://www.intuit.ru/studies/courses/6/6/lecture/184?page=5
18. Программное обеспечение SPSS [Электронный ресурс] /URL:http://www-01.ibm.com/software/ru/analytics/spss/
19. Dan Pelleg Accelerating Exact k-means Algorithms with GeometricReasoning / Dan Pelleg, Andrew Moore // Carnegie Mellon University,Pittsburgh.–2010.
20. Harry Zhang The Optimality of Naive Bayes / Harry Zhang // University ofNew Brunswick Fredericton, New Brunswick, Canada–2014.
21. БенкенЕ.С. PHP, MySQL, XML.Программированиедля Интернета[Текст]–СПб.: БХВ-Петербург, 2011.
22. TIOBE Programming Community Index for November 2013 [Электронныйресурс]
23. Щерба М.А. Обнаружение низкоактивных распределенных атак типа«Отказ в обслуживании» в компьютерных сетях: дис. ... работа канд. тех.наук Омский гос. университет, Омск, 2012.
24. Терновой О.С. Обнаружение источников вредоносного трафика DDoS-атак методами статистического анализа. В кн.: МатериалыXV Региональной конференции по математике, Барнаул, июнь, 2012. С. 80
25. Debian[Электронныйресурс]/URL:http://www.debian.org/index.ru.html
26. Сразу у нескольких новостных алтайских сайтов возникли технические проблемы [Электронный ресурс] /URL: http://amic.ru/news/183654/
27. Диаграмма мощности DDoS-атак [Электронный ресурс] /URL:http://www.securelist.com/ru/images/vlill/ddos_sept2013_pic08.png

28. Сайт amic.ru подвергся DDoS-атаке [Электронный ресурс] /URL:http://www.amic.ru/news/192772/

29. MittaI, P. Defense against Distributed Denial of Service Attacks : a seminar report.–Department of Computer Science and Engineering. Indian Instituteof Technology, 2015.–20 p

30. MirkovicJ. A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms :Technical report #020018 I J. Mirkovic, J. Martin, P. Reiher.–ComputerScience Department. University of California, 2002.–16 p

31. DNSAmplificationAttacks[Электронныйресурс]/URL:http://www.securiteam.com/securityreviews/5GP0L00I0W.html

32. Amazon Elastic Compute Cloud [Электронныйресурс] / URL:http://aws.amazon.com/ec2/

33. Erik Nygren The Akamai Network: A Platform for High-PerformanceInternet Applications Ramesh K. Sitaraman, and Jennifer Sun.–ACMSIGOPS Operating Systems Review, vol. 44, no. 3, July 2010.

34. Cabrera, J.B.D. Proactive detection of distributed denial of service attacksusing mib traffic variables–a feasibility study I J.B.D. Cabrera, L. Lewis, X.Qin et al. II Proc.of International Symposium on Integrated NetworkManagement. Seattle, 14–18 May. 2011.–Piscataway: IEEE, 2001.–P. 609–622.

35. Joannidis, J. Implementing Pushback: Router-Based Defense Against DDoSAttacksIJ. loannidis, S.M. BellovinIIProc. of Symposium of Network andDistributed Systems Security (NDSS). San Diego,6-8February2012.-[S.1.: s.n.],2012.-P.57-71.

36. Manajan, R. Controlling High Bandwidth Aggregates in the Network : ICSITechnical ReportIR. Manajan, S.M. Bellovin, S. Floyd et al.-ICSI,2011.-16

37. CoIIins, M. An Empirical Analysis of Target-Resident DoS Filters I M.Collins, M.K. Reiter If Proc. of 2014 IEEE Symposium on Security andPrivacy (S&P'04). Oakland, May9–12,2014.–Piscataway : IEEE, 2004.–P. 103–114.

38. ЩербаЕ.В.Разработка системы обнаружения распределенных сетевыхатак типа «Отказ в обслуживании»/Щерба Е.В., Волков Д.А.//«Прикладная дискретная математика. Приложение».–2013. No6–С.68-70.

39. Никишова А.В.Обнаружение распределенных атак наинформационную систему предприятия/Никишова А.В., Чурилина А.Е.// «Известия Южного федеральногоуниверситета. Технические науки».–2013. No12(149)–С.135–143.

40. Корнев Д.А.Активные методы обнаружения SYN-floodатак/КорневД.А., Лопин В.Н., Лузгин В.Г.// «Информационная безопасность».–2012.Т. 15,No2– С.189–196.
41. IBMProventia Network Intrusion Prevention System(IPS) [Электронный ресурс]/URL:http://www.ibm.com/ru/services/iss/proventia_network_intrusion_prevention.html
42. Cisco Guard DDoS Mitigation Appliances [Электронныйресурс] / URL:http://www.cisco.com/web/RU/products/ps5888/index.html
43. KasperskyDDoSPrevention[Электронныйресурс]/URL:http://www.kaspersky.ru/ddos-prevention
44. CloudFlare [Электронный ресурс] /URL:https://www.cloudflare.com/
45. Iptables Tutorial1.2.2 [Электронный ресурс] /URL: https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html
46. DDOS Deflate[Электронныйресурс]/URL:http://deflate.medialayer.com/
47. mod_evasive–защита отDOSиDDoS-атак [Электронный ресурс] /URL:http://muff.kiev.ua/content/modevasive-zashchita-ot-dos-i-ddos-atak
48. Модуль ngx_http_limit_zone_module[Электронный ресурс] /URL:http://nginx.org/ru/docs/http/ngx_http_limit_zone_module.html
49. Простой способ защиты от классического HTTP DDoS [Электронный ресурс] /URL:http://habrahabr.ru/post/151420
50. Эдгар Э. Петерс Хаос и порядок//Э.Э. Петерс–Москва: Мир, 2010–85с.
51. Названы имена победителей конкурса «Лучшие проекты информатизации–2013» [Электронный ресурс] /URL:http://www.it-alttpp.ru/news/forumnews/2013/10/07/782/
52. Афанасьев А.DDOS: противостояние. Как происходят атаки и как ихотражать // Системный администратор. Синдикат 13. М.–2011. No1.–2(122–123).– С. 59–61.
53. Sigmond S. DDOS attacks: precursor to digital terrorism // SIGMOND S.,KAURA V. // SILICONINDIA–2011.Т. 5. No11.–С.60–62.
54. Поисковая система mnoGoSearchдляWindows–русская версия[Электронный ресурс] /URL:http://www.mnogosearch.org/winrus.html

ПРИЛОЖЕНИЕ

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;

namespace KNN
{
   public class Pair: IComparable
   {
      public double Y;
      public double Distance;

      public Pair(double y, double distance)
      {
         Y = y;
         Distance = distance;
      }
      public int CompareTo(object other)
      {
         return Distance.CompareTo(((Pair)other).Distance);
      }
   }
   public class XY : IComparable<XY>
   {
      public double X;
      public double Y;

      public XY(double x, double y)
      {
         X = x;
         Y = y;
      }
      public int CompareTo(XY other)
      {
         return X.CompareTo(other.X);
      }
   }
   public class MaxPQ<Key> where Key : IComparable
   {
      private Key[] pq; // heap-ordered complete binary tree
      private int N = 0; // in pq[1..N] with pq[0] unused
      private int maxCapacity;
      public MaxPQ(int maxN)
      {
         maxN++;
```

```
        pq = new Key[maxN + 1];
        maxCapacity = maxN;
    }
    public bool isEmpty()
    { return N == 0; }
    public int size()
    { return N; }
    public void insert(Key v)
    {
        pq[++N] = v;
        swim(N);
        if (N == maxCapacity) delMax();
    }
    public Key delMax()
    {
        Key max = pq[1]; // Retrieve max key from top.
        exch(1, N--); // Exchange with last item.
        //pq[N+1] =  null; // Avoid loitering.
        sink(1); // Restore heap property.
        return max;
    }

    private bool less(int i, int j)
    { return pq[i].CompareTo(pq[j]) < 0; }
    private void exch(int i, int j)
    { Key t = pq[i]; pq[i] = pq[j]; pq[j] = t; }
    private void swim(int k)
    {
        while (k > 1 && less(k / 2, k))
        {
            exch(k / 2, k);
            k = k / 2;
        }
    }
    private void sink(int k)
    {
        while (2 * k <= N)
        {
            int j = 2 * k;
            if (j < N && less(j, j + 1)) j++;
            if (!less(k, j)) break;
            exch(k, j);
            k = j;
        }
    }
}}
```