УДК 004.9

ОБЗОР МЕТОДОВ И ИНСТРУМЕНТОВ ДЛЯ РЕАЛИЗАЦИИ РАСПРЕДЕЛЕННЫХ АТАК ОТКАЗА В ОБСЛУЖИВАНИИ

© 2017 М. С. Бондаренко

Воронежский институт высоких технологий (г. Воронеж, Россия)

Распределенные атаки отказа в обслуживании (DDoS) являются наиболее распространенным и самым эффективным средством в арсенале злоумышленников. Атаки такого вида имеют широкий спектр областей применения, а так же подходов и средств для их реализации. Распределенные атаки отказа в обслуживании могут быть направлены на верхние четыре уровня эталонной модели OSI. Цель DDoS-атак заключается в исчерпании вычислительных или канальных ресурсов системы, тем самым лишая легитимных пользователей возможности использования сервисов этой системы. Классическим подходом в реализации DDoS-атаки является использование масштабных сетей, состоящих из сотен тысяч зараженных устройств, что позволяет скрыть личность злоумышленника.

Ключевые слова: DDoS, атака, ботнет, HTTP-флуд, SYN-флуд, Slowloris.

Распределенные атаки, направленные на отказ в обслуживании (DDoS).

В настоящее время все чаще в СМИ появляются сообщения о совершении атак направленных на отказ в обслуживании. Целью таких атак являются сервисы государственных органов, а так же крупных компаний и предприятий. Помимо этого атакам подобного рода подвержены инфраструктуры городов и целых стран, такие как энергетика, связь, регулирование дорожного движения и прочие сферы управляемые с помощью серверного вычислительного оборудования.

Чаще всего DDoS атаки используются злоумышленниками с целью заявить о собственном существовании в знак протеста политике страны или отдельной компании, или же снизить лояльность пользователей сервисов компании, ведущих к прямым финансовым убыткам. Но нередко атаки подобного рода используются как прикрытия основных действий злоумышленника. В то время пока специалисты по сетевой безопасности направляют усилия на отражение атаки и восстановление штатной работы сервисов, происходит кража секретной информации, денежных средств, или же заражение инфраструктуры атакуемого объекта с целью дальнейшего шпионажа или контроля.

DdoS-атака в первую очередь — это средство конкурентной борьбы. Для реализации подобного рода атак злоумышленники чаще всего используют сети из зараженных компьютеров или портативных устройств, которые называют ботнетами. Ботнеты состоят из сотен и тысяч зараженных компьютеров по всему миру, владельцы которых могут даже не подозревать, что с помощью их компьютеров совершаются противозаконные действия. Согласно исследованиям представленным лабораторией Касперского, наибольшее количество зараженных машин, которые входят в ботнеты, находится на территории Российской Федерации.

Ботнеты позволяют скрыть личность истинного злоумышленника, поскольку атака производится со сторонних компьютеров со всего мира, и часто такой подход используется для атак государственного уровня, когда зараженные компьютеры, расположенные в одной стране, совершают атаку на вычислительные сервисы другой страны.

Основные сценарии атак отказа в обслуживании бывают двух видов. Принципом первого вида атак является исчерпание операционных ресурсов сервера, таких как ресурсы процессора и оперативной памяти, а так же методы записи информации на жесткие диски после которых запись на них перестает быть возможной. Вторым видом атак отказа в облуживании является исчерпание канальных ресурсов сети, при котором легитимные пользователи просто не смогут подключиться к серверу, так как канал связи будет перегружен. Среди объектов атаки можно выделить:

1. Уровень приложений.

Бондаренко Михаил Сергеевич – Воронежский институт высоких технологий, магистрант, mikhailbondarenko2017@yandex.ru.

• Веб-приложения или любой из их компонентов (СУБД, сервер аутентификации).

• Сервисы, обеспечивающие работу прикладного уровня инфраструктуры (например, DNS).

• Приложения, обеспечивающие бизнес-процессы.

2. Сетевой и транспортный уровни.

На данных уровнях злоумышленник может эксплуатировать архитектурные уязвимости протоколов IP, ICMP, TCP, UDP, а так же уязвимости в методах работы конкретной операционной системы с этими протоколами.

Сценарии DDoS атак (ICMP, UDP, SYN) – flood. Принципы такого рода атак аналогичны, поэтому для понимания принципа рассмотрим такой сценарий на примере SYN-flood атаки.

SYN-flood атака реализуется на основе правила о трехстороннем рукопожатии, при котором клиент отправляет серверу пакет, который содержит SYN – флаг, сообщая серверу о начале сеанса. На этот пакет сервер отвечает SYN-ACK пакетом, которым подтверждает клиентское подключение и открывает обратный порт соединения, после чего ожидает ACK – пакета от клиента для подтверждения обратного сеанса и завершения трехстороннего рукопожатия.

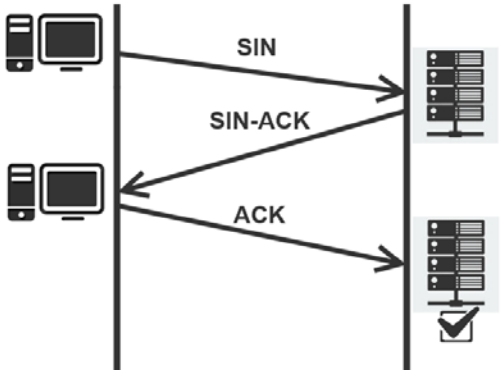

Рисунок 1. Схема трехстороннего рукопожатия.

В случае же атаки злоумышленник отправляет множественные пакеты SYN, не подтверждая обратные запросы сервера, вследствие чего сервер вынужден ожидать подтверждения сеанса, сохраняя соединение в памяти, которая ограничена. При заполнении стека подключения на сервере, легитимные клиенты не смогут открыть соединение с сервером, ввиду чего сервис станет недоступным. Единственным отличием ICMP и UDP атак такого рода, является их направленность не на вычислительные ресурсы сервера, а на канал связи.

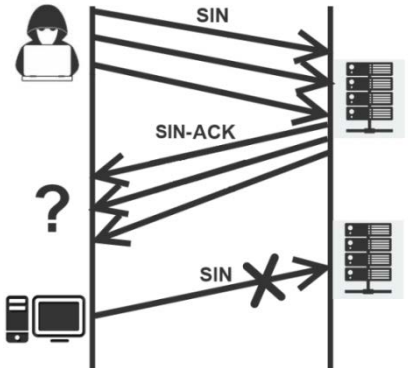

Рисунок 2. Схема реализации SYN-flood атаки.

Атаки на канал связи зачастую имеют меньшую популярность из-за большой разницы в ресурсах атакующей и защищающейся стороны. Поскольку у крупней серверные фермы и дата-центры имеют зачастую довольно широкий канал связи, для перегрузки которого злоумышленнику понадобятся намного больше вычислительных ресурсов чем для атак на серверные вычислительные ресурсы.

Наибольшую популярность имеют атаки отказа в обслуживании направленные на уровень приложений, в частности HTTP-flood. Поскольку в данной ситуации злоумышленники имеют большее отношение ресурсов необходимых атакующей стороне, к ресурсам необходимым на стороне приложения.

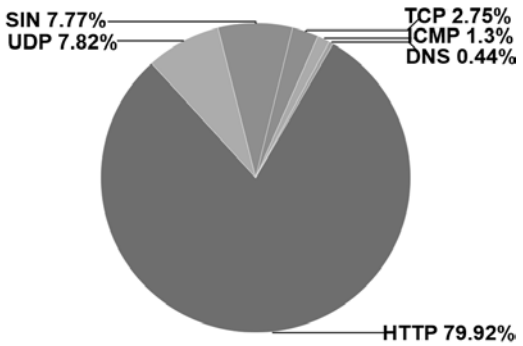

Рисунок. 3. Популярность видов DDoS-атак.

Классическим примером HTTP-flood атаки является атака Slow POST (Slowloris), которая была обнаружена в 2009 году, и на момент обнаружения перед ней были уязвимы практически все веб-серверы. Основной причиной этого послужила эксплуатация уязвимости веб-серверов Apache на архитектурном уровне, что не позволяло разработ-

чикам платформы в короткие сроки выпустить обновление закрывающее уязвимость.

Основным принципом атаки Slowloris является возможность отправки пакета, содержащего заголовок с длинной контента (Content-Length), при получении которого сервер будет ожидать данные от клиента, отправившего пакет. В заголовке указывается размер пакета данных в байтах, который будет ожидать сервер. Реализация атаки заключается в множественном подключении к серверу и медленной побайтовой отправке определенного в пакете количества данных, тем самым затрачивая пул подключений веб-сервера.

С развитием истории вычислительной техники выяснилось, что результат распределенного решения одной и той же задачи с помощью нескольких компьютеров не уступает в скорости решения задачи традиционным суперкомпьютером, но в свою очередь требует гораздо меньших финансовых и производственных затрат на проектирование реализацию и обслуживание. Таким образом, появились сети распределенных вычислений (Grid – сети), которые первоначально использовались для решения математических задач, расчета криптографических функций, при синтезе новых видов лекарств и так далее. Но также подобного рода сети стали использовать злоумышленники, создавая ботнеты для реализации распределенных DDoS-атак.

На сегодняшний день существует два типа ботнетов.

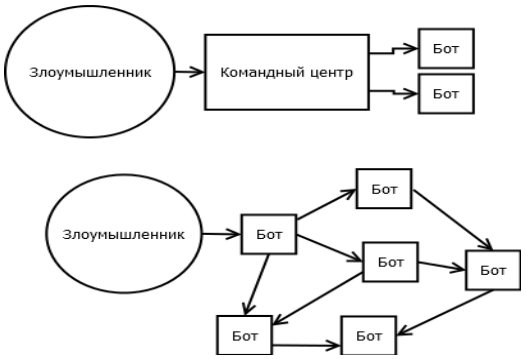

Рисунок 4. Подходы к реализации ботнетов.

1. Первый тип ботнета C&C – это ботнет, имеющий командный центр, к которому злоумышленник заставляет подключаться зараженные компьютеры. Впоследствии боты получают от него команды на выполнение атак. Сам же злоумышленник подключается к командному центру и оставляет на нем команды для ботов. Существуют различные способы реализации командного центра, например веб-сайт, на страницах которого размещены команды для ботов, или же создается канал в IRC-чате, к которому подключаются боты и получают команды в виде сообщений. Но в настоящее время наибольшее распространение получила реализация командного центра основанного на популярных веб-сервисах. Для создания такого командного центра злоумышленнику достаточно создать аккаунт в социальной сети, на котором размещаются команды для ботов. Боты в автоматическом режиме подключаются к этому аккаунту, считывают команды и начинают их выполнять. Преимущество такого вида командного центра заключается в том, что у злоумышленника больше нет необходимости заботиться о нагрузке на свой командный центр, так как платформой являются серверы социальной сети предусмотренной на множественное подключение пользователей.

Среди недостатков C&C – архитектуры можно выделить:

• Плохая масштабируемость – с ростом числа зараженных компьютеров возрастает нагрузка на командный центр, вследствие чего может произойти обратная DDoS-атака на командный центр, когда количество подключаемых ботов превысит количество ресурсов командного центра.

• Централизованное управление чревато высокой вероятностью обнаружения и изолирования командного центра, что немедленно прекратит работу всего ботнета.

2. Исходя из недостатков C&C-архитектуры, была создана распределенная P2P-архитектура, в которой злоумышленник подключается к одному из ботов и размещает на нем команды для всех ботов, после чего боты автоматически распространяют команды между собой. У этой архитектуры также есть ряд недостатков:

• уведомление каждого бота о существовании других зараженных машин;

• дополнительные порты для получения и передачи команд на стороне бота, что может быть чревато определением и блокировкой вредоносного программного обеспечения антивирусным программным обеспечением;

• время, затрачиваемое на передачу команд между ботами;

• трудность ведения статистики, которая собирает информацию об общем количестве ботов в ботнете.

По причине большого количества недостатков, злоумышленники придумали но-

вый способ реализации командного центра, сохраняя все преимущества централизованной архитектуры, но при этом обеспечивая анонимность командного центра. Для этого был создан такой инструмент как генерация доменов. Принцип работы этого инструмента заключается в размещении на всех ботах генераторов псевдослучайных чисел. В случае отказа соединения с текущим доменом командного центра, бот начинает генерировать новый домен. Обладая аналогичным генератором, злоумышленник может понять, в какой момент времени какой домен сгенерирует бот, и в случае отсутствия доступа к командному центру, злоумышленник знает, к какому домену будет подключаться бот и может заранее разместить на нем необходимые команды [1].

Классическим развитием DDoS-атаки является захват различных компьютеров и портативных устройств в один общий ботнет, и проведение стандартного SYN, ICMP, HTTP-flood. Такие атаки встречаются и в нынешнее время, но тренды проведения распределенных атак отказа в обслуживании постепенно меняют свой вектор. Несколько лет назад был обнаружен новый подход, в котором использовались не вычислительные ресурсы ботнета, а большое количество, расположенных на хостинге с широким каналом, веб-сайтов. Классическим проявлением такой атаки является атака на уровень приложений, а в частности HTTP-flood.

Сегодня же с приходом в наш обиход облачных технологий, злоумышленники используют не только ботнеты в привычном их понимании, но и вычислительные средства облачных ресурсов. С помощью облачных технологий злоумышленник может создать тысячи виртуальных ботов с необходимыми параметрами. При такой реализации у злоумышленника больше нет необходимости обслуживать свой ботнет, и распространять вредоносное программное обеспечение. Одним из самых новых решений в реализации DdoS-атак является синтез вычислительных ресурсов, предоставляемых облачными технологиями, с Amplification-атаками. Amplification-атаки направлены на усиление получаемых пакетов и отправке их жертве. Наиболее распространенным сценарием является DNS-Amplification, основанный на протоколе DNS, при реализации этого сценария злоумышленники используют классический или облачный ботнет для отправки сотен тысяч запросов к уязвимым DNS-ресурсам. Уязвимые DNS-ресурсы усиливают полученные пакеты в несколько раз, тем самым эмитируя нагрузку на ресурс жертвы в сотни тысяч ботов, при этом, не обладая такими ресурсами. Однако и такие технологии реализации атак не идеальны, поэтому рассмотрим вероятные методы развития DDoS-атак в будущем.

Облачные технологии принесли нам такое понятие как SaaS (software as a service), которое означает переход привычного всем программного обеспечения в веб-пространство. По такому принципу на веб-платформу перешел и инструмент веб-разработчиков JMeter, который предназначен для имитации нагрузки на веб-ресурс с заданным количеством подключений. Злоумышленник может использовать такие инструменты нагрузочного тестирования для осуществления DDoS-атак, и при этом у него появляется несколько преимуществ:

1. Поскольку ресурс для тестирования не позиционируется как инструмент для атак, его трафик считается легитимным, поэтому распознать трафик от нагрузочного сервера намного сложнее, чем от обычного ботнета.

2. Интеллектуальный трафик – эта технология позволяет задать нагрузочному серверу сценарий поведения типичного пользователя ресурса, например переход по определенным страницам сайта и запуск платежной системы. Такой трафик крайне трудно отличить от пользовательского трафика, что усложняет обнаружение атаки.

3. Веб-сервисы тестирования не проверяют владельца сайта – это значит то, что инструментами нагрузочного тестирования может воспользоваться любой пользователь против любого сервиса.

4. Анализ на предмет «тяжелого» контента – эта технология нагрузочных сервисов предоставляет злоумышленнику информацию о наиболее «тяжелом» контенте сайта, с помощью обращения к которому удастся гораздо быстрее исчерпать ресурсы веб-сервера.

Примером такого нагрузочного сервиса является Loadimpact.com, который позволяет произвести большую нагрузку на веб-ресурс, а так же узнать наиболее уязвимые места сервиса с точки зрения контента.

Злоумышленники могут использовать концепцию SaaS в корыстных целях, они могут использовать любой ресурс, который так или иначе может обратиться к целевому ресурсу, как средство для усиления ботнета. Примером такого подхода могут являться

Whois-сервисы, предназначенные для получения справочной информации о владельце какого либо сайта, при этом сервис сам будет обращаться к этому сайту. Таким образом, злоумышленник может запросить данные о жертве у Whois-сервиса с тысяч компьютеров своего ботнета, тем самым существенно увеличив нагрузку на конечный сайт со стороны Whois-сервиса.

Методы защиты от DDoS-атак.

1. Резервирование критичных ресурсов

2. Выполнение требований стандартов безопасности (NIST)

3. Регулярное проведение нагрузочных тестирований и правильное инвестирование денег в средства защиты.

ЛИТЕРАТУРА

1. Денис Макрушин Искусство зомбирования: Азбука создания неугоняемых ботнетов – https://xakep.ru/2010/08/07/54478/.

REVIEV METHODS AND TOOLS FOR IMPLEMENTATION OF DISTRIBUTED DENAL OF SERVICE ATTACKS

© 2017 M. S. Bondarenko

Voronezh Institute of High Technologies (Voronezh, Russia)

Distributed denial of service (DDoS) are the most common and most effective tool in the arsenal of criminals. Attacks of this kind have a wide range of applications, as well as approaches and tools for their implementation. Distributed denial of service attack can be directed to the upper four layers of the OSI reference model. The goal of DDoS-attacks is exhausted computing system or channel resources, thereby depriving the legitimate users the possibility of using the services of this system. The classic approach in the implementation of DDoS-attacks is the use of large-scale networks consisting of hundreds of thousands of infected devices that allows you to hide the identity of the attacker.

Key words: DDoS, attack, botnet HTTP-flood, SYN-flood, Slowloris.