УДК 004.7

Р.И. Шумский
Донецкий национальный технический университет, г. Донецк
кафедра компьютерной инженерии

АНАЛИЗ РАСПРЕДЕЛЁННЫХ СЕТЕВЫХ АТАК И МЕТОДОВ ЗАЩИТЫ

Аннотация

Шумский Р.И. Анализ распределённых сетевых атак и методов защиты. *В данной статье рассматриваются различные типы сетевых атак типа DDoS, причины их возникновения. Описаны основные методы и способы борьбы с данным видом атак. Приведена статистическая информация, показывающая текущую ситуацию в вопросах обеспечения стабильной работы информационных систем и сетей.*

Ключевые слова: *DDoS-атака, распределённая сетевая атака, использование эксплоитов, флуд, полезная нагрузка.*

Постановка проблемы. Одной из актуальных задач в сфере услуг предоставления информации является обеспечение стабильной работы и возможности доступа к базам данных в любое время. При работе в таком режиме так же необходимо обеспечение определённой степени надежности и стрессоустойчивости системы. DDoS-атака (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании») является одной из наиболее серьёзных и распространённых. Ее цель - доведение системы до отказа, то есть, создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам, либо этот доступ оказывается затруднён.

Анализ литературы. В учебных курсах данная тема охватывается слабо, однако большое количество информации можно найти в свободном доступе в различных статьях [1] на сайтах ведущих компаний (например, таких, как [2]). В данных статьях предоставляются актуальная статистическая информация, рассматриваются методы, которые были использованы в реальных атаках, проводится анализ, и выдвигаются определённые рекомендации для противостояния атакам в будущем.

Цель статьи – рассмотреть причин возникновения DDoS-атак и способов их создания, а также выполнить анализ методов борьбы с DDoS-атаками для последующего выбора наиболее эффективных.

Анализ современной ситуации борьбы с сетевыми атаками. Согласно отчёту, опубликованному компанией Arbor Networks [4], предоставляющей одни из лучших решений для обеспечения стабильной работы информационных систем и имеющей огромный опыт в вопросах борьбы с DDoS-атаками, в 2012-ом году рост количества и интенсивности атак замедлился по сравнению с предыдущими годами. При этом комплексные атаки и атаки уровня приложений продолжают развиваться, становясь более сложными. По результатам анализа компании 46% атак относились к комплексным DDoS-атакам, использующим отправку мусорного трафика, SYN-флуд (отправка большого количества запросов на подключение по протоколу TCP) и UDP Flood (отправка большого количества множества UDP-пакетов), а так же к атакам с использованием протоколов уровня приложений (они стали наиболее распространёнными и составили порядка 85% от вышеперечисленных). Однако, по сравнению с предыдущими годами пропорции заявленных атак этого типа практически не изменились по отношению к большинству служб, таких как HTTP, DNS и SMTP. Единственным аспектом атак уровня приложений, который явно пережил изменение, стал HTTPS-протокол, уровень применения которых поднялся с 24% до 37%.

Согласно отчёту, существует определённая обеспокоенность по поводу компрометации рабочих станций. Существует вероятность того, что компьютеры, принадлежащие к корпоративной сети, могут быть частью ботнета (сеть из зараженных компьютеров, которые используются в атаке). Такая ситуация приводит к усилению эффекта от атаки, так как защита может быть направленна только на внешнюю сеть, игнорируя внутрисетевой корпоративный трафик.

Увеличение количества хостов, входящих в ботсети, не вызывает удивления, учитывая количество и сложность существующих на сегодняшний день вирусов, темпы их развития и исходящую из этого невозможность построить надежную систему защиты на основе антивирусных программ и систем обнаружения вторжений.

Самой сильной DDoS-атакой за 2012-й год оказалась атака, которая обрушилась на сервера компании Cloudflare 15-го сентября. В результате сервис Cloudflare оказался временно недоступен для части пользователей. Стоит заметить, что компания является сетью доставки контента и под её управлением находится несколько центров данных в разных регионах. Компания легко выдерживает DDoS-атаки в десятки гигабит, но с атакой в 65 Гбит/с справиться не смогла.

В марте 2013 года компания Spamhaus, которая формирует базы данных о серверах, используемых хакерами, что помогает почтовым службам фильтрации спама и другого нежелательного контента, занесла в свой чёрный список ряд серверов, принадлежащих голландской компании CyberBunker. Компания CyberBunker заявила, что Spamhaus не имеет права указывать, что

публиковать и что не публиковать в интернете. Голландская компания развернула самую мощную DDoS-атаку за всё время. Её мощность достигала 300 Гбит/с. Но атака даже такой мощности не смогла нанести большого вреда, так как была задействована технология защиты, а именно: распределение трафика по различным дата-центрам и последующая его фильтрация.

Эта атака имела определённое воздействие на всю сеть Интернет, что было выражено в увеличении пинга до некоторых европейских сайтов. Провайдеры нормально выдержали атаку, но были сильно зафлужены.

Причины возникновения DDoS-атаки. По сложности подавления и мотивации проведения DDoS-атаки можно разделить на следующие категории.

1) Вандализм. Обычно это не распределенные атаки, а атаки, которые ведутся с одного-двух хостов, злоумышленник скорее всего не получает от атаки финансовой выгоды, а делает это из-за обиды на владельцев какого либо ресурса. Знания его в этой области ограничены простыми методами атак, найденными в сети Интернет. Данные атаки отражаются достаточно легко, так как тоже не требуют высокой квалификации в области защиты компьютерных сетей от внешних атак. Зачастую достаточно блокировать конкретный IP или выполнить простую фильтрацию пакетов по замеченной закономерности.

2) Нигилизм. Причины действий, фактически, идентичны предыдущему типу, но действия происходят более целенаправленно. Это уже распределенная атака. В ней участвует группа людей, которая недовольна теми или иными информационными поводами. Обычно, это простой bat-скрипт, в котором используется команда ping с большим размером проверочного пакета и перечислены атакуемые ресурсы. Никаких знаний от пользователя не требуется, достаточно лишь запустить скрипт. Блокируется такая атака обычно достаточно легко, т.е. блокируется вся информация, полученная по протоколу ICMP. Бизнес – злоумышленники используют данный вид атак не только как средство для собственного обогащения, но и предоставляют организацию такой атаки в качестве услуги.

Анализ DDoS-атаки. Рассмотрим принципы, по которым была произведена самая мощная атака (рис.1). Согласно отчёту [5], в основе данной атаки лежит UDP-флуд, который сопровождается SYN-флудом. Это указывает на наличие достаточно большого числа подконтрольных серверов.

Так же в ходе данной атаки была использована технология усиления атаки. Умножение первоначального вредоносного трафика осуществлялось за счёт отражения DNS-запросов через DNS-приемники, которые установлены у каждого интернет-провайдера. Обычно DNS-приемники сконфигурированы таким образом, чтобы обрабатывать только запросы своих пользователей. Но существует также большое количество компаний, в которых из-за неправильной конфигурации принимаются запросы от любого пользователя интернета. В значительной мере усиление происходило благодаря большим

ключам DNSSEC, которые включены в тело ответа, а ведь протокол DNSSEC внедрялся с целью повысить безопасность системы DNS.

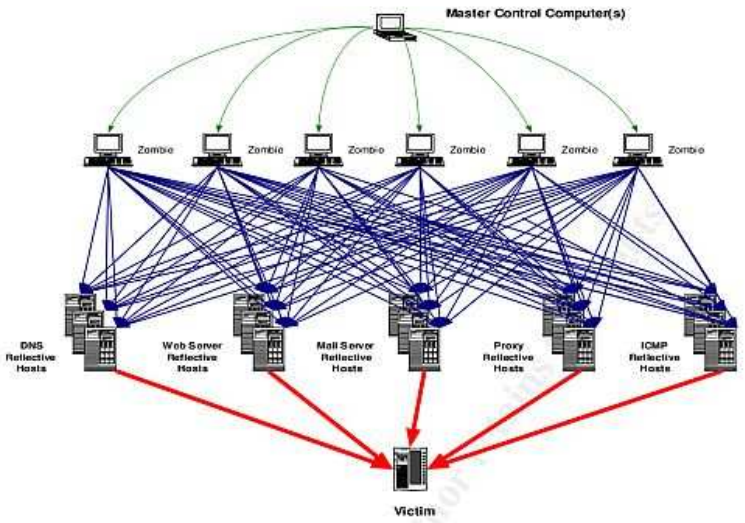

Рисунок 1 – Пример типичной DDoS-атаки

Защита от DDoS-атак. Существуют основные решения по защите от атак:

- программные решения;
- аппаратные решения;
- облачные решения.

Программные решения – самое распространённое на рынке, зачастую представляет собой набор правил фильтрации трафика, которые составлены разработчиком на личном опыте. Данное решение достаточно просто установить прямо на сервер, на котором работает ресурс, но оно поможет только от малозаметных атак вида «вандализм».

Аппаратные решения представляют собой создание распределённой сетевой структуры с большим запасом пропускаемого трафика. Используются в масштабных сетевых структурах, таких как: точки обмена трафиком, дата-центры, крупные региональные провайдеры.

Облачные решения представляют из себя сетевую структуру с большой пропускной способностью, в состав которой вводятся сервера для фильтрации вредоносного трафика. Таким образом, такая сеть постепенно будет отфильтровывать негативный трафик и снижать количество вредоносных пакетов. Анализ трафика является достаточно сложной задачей, поэтому некоторые компании патентуют свои алгоритмы, например компания “Black Lotus” запатентовала алгоритм «Human Behavior Analysis». Этот алгоритм

определяет, кто генерирует трафик, человек или бот. Компания «Arbor» предоставляет свой продукт «PeakFlow», который имеет сигнатурный подход к фильтрации нежелательного трафика.

Выводы

В статье рассмотрены причины возникновения DDoS-атак, их мотивация и способы создания. Показано, что данная проблема на сегодняшний день является актуальной. Существуют явные лидеры рынка в данной области, но они предоставляют закрытые решения, которые защищены патентом или совсем не разглашаются. В отличие от решений с закрытым исходным кодом, открытые рекомендации позволяют привести методики и алгоритмы к единому стандарту, что позволит производителям оборудования и программных решений обмениваться средствами более эффективного решения данной проблемы.

Список литературы

1. DDoS and Security Reports: The Arbor Networks Security Blog – http://ddos.arbornetworks.com/2012/09/understanding-the-nature-of-ddos-attacks/
2. Сайт Лаборатории Касперского - http://www.securelist.com/ru/analysis
3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 4 издание, 2010, 943с.
4. Статистика глобальной сетевой активности - http://atlas.arbor.net/summary/attacks
5. Самая крупная DDoS-атака в истории - http://www.xakep.ru/post/60356/
6. Дядин И.П. Исследование распределённых информационных атак – http://ea.donntu.edu.ua:8080/jspui/bitstream/123456789/16061/1/%D0%94%D1%8F%D0%B4%D0%B8%D0%BD_%D0%A7%D0%B5%D1%80%D0%B2%D0%B8%D0%BD%D1%81%D0%BA%D0%B8%D0%B9.pdf