УДК 004.492.4

Нурекен Е.Н., Радченко Д.А., магистранты
Алматинского Университета Энергетики и Связи имени Гумарбека Даукеева

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ ПОДХОДОВ К ЗАЩИТЕ ОТ DDOS-АТАК

DDOS ШАБУЫЛДАРЫНАН ҚОРҒАУДЫҢ ЗАМАНАУИ ТӘСІЛДЕРІН ЗЕРТТЕУ

RESEARCH OF MODERN APPROACHES TO PROTECTION AGAINST DDOS ATTACKS

Аннотация. В этой статье излагаются исследование современных подходы к защите от DDoS - атак «Распределенный отказ в обслуживании». DDoS-атака — это довольно популярный тип атаки, направленный на ограничение доступности Интернет-сервисов и ресурсов. DDos-атака может исходить из любой точки сети и обычно подавляет сервер жертвы отправкой огромного количества трафика. На начало 2020 года существует множество подходов к защите от данного типа атак. В данный статье будут рассмотрены последние новшества в защите от DDOS – атак. А также изложен практический опыт, накопленный авторами данной статьи.

Ключевые слова: Распределенный отказ в обслуживании, DDoS – атака, компьютерные сети, информационная безопасность, интернет-сервисы, серверы СУБД, непрерывность бизнес-процессов, система идентификации вторжений.

Abstract. This article outlines a study of current approaches to defending against Distributed Denial of Service (DDoS) attacks. DDoS attack is a fairly popular type of attack to restrict the availability of Internet services and resources. A DDos attack can come from anywhere on the network and usually overwhelm the victim's server by sending a huge number of packets. As of early 2020, there are many approaches to defending against this type of attack. This article will review the latest innovations in protection against DDOS attacks. It also describes the practical experience accumulated by the authors of this article.

Keywords: Distributed denial of service, DDoS - attack, computer networks, information security, Internet services, DBMS servers, business continuity, intrusion identification system.

Аңдатпа. Бұл мақалада «Қызметтен бас тарту» (DDoS) шабуылдарынан қорғанудың қазіргі тәсілдерін зерттеу көрсетілген. DDoS шабуылы - бұл Интернет қызметтері мен ресурстарының қол жетімділігін шектейтін шабуылдың танымал түрі. DDos-шабуыл желідегі кез-келген жерден болуы мүмкін және әдетте көптеген пакеттерді жіберу арқылы құрбанның серверін басып алады. 2020 жылдың басынан бастап шабуылдың осы түрінен қорғанудың көптеген тәсілдері бар. Бұл мақалада DDOS шабуылдарынан қорғаудың соңғы жаңалықтары қарастырылады. Сондай-ақ, осы мақала авторлары жинақтаған практикалық тәжірибе сипатталған.

Түйін сөздер: Қызметтен бас тарту, DDoS - шабуыл, компьютерлік желілер, ақпараттық қауіпсіздік, Интернет қызметтері, ДҚБЖ серверлері, бизнестің үздіксіздігі, кіруді анықтау жүйесі.

Введение. С появление первых интернет-ресурсов и распространению глобальной сети интернет вопрос интернет-безопасности вышел на абсолютно новый уровень. 22 июля 1999 года можно считать важной датой в истории информационной безопасность. Ведь именно в данный день была зафиксирована первая DDOS-атака. Она была направлена на

один из компьютеров Миннесотского университета. Эта атака была осуществлена со стороны сети, состоящей из 114 компьютеров, зараженных вирусом «Trin00». В дальнейшем такие сети стали называть «botnets». Еще одна атака была осуществлена против Yahoo! в феврале 2000 г. 20 октября 2002 г., еще от одной DDoS-атаки пострадали 13 корневых серверов, отвечающих за предоставление системы доменных имен (DNS). Распределенный отказ в обслуживании (DDoS) атака — это атака, направленная на то, чтобы помешать пользователям использовать ресурсы веб-сервера жертвы. Данная атака осуществляется посредством так называемой бот-сети (botnets). «Botnets» в своем классическом представлении состоит из Атакующего - хакера, «Мастера» - удаленный взломанный компьютер (управляется хакером), «Зомби-демоны» - зараженные компьютеры входящие в состав «botnets» управляемые «Мастером» рис. 1.

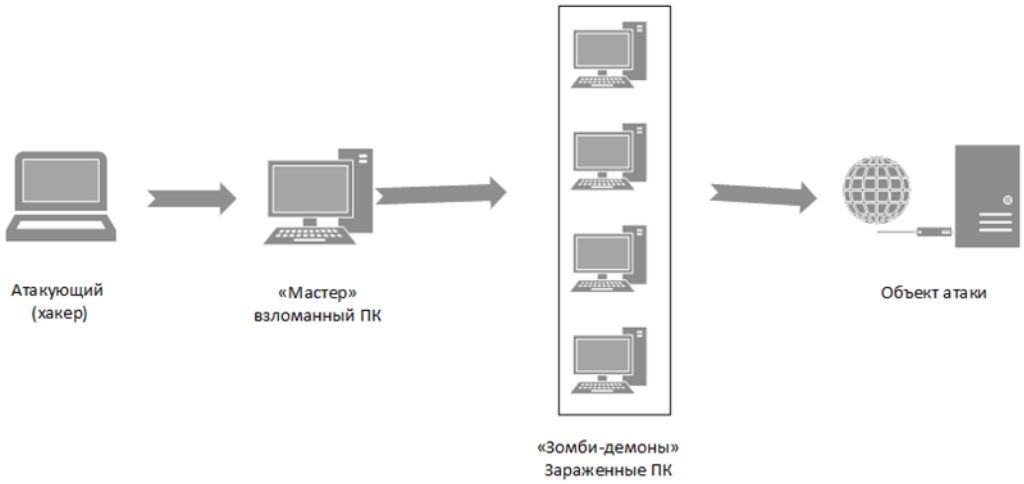

Рисунок 1. Схема стандартной DDoS-атаки.

Данный вид атака относится к антропогенному типу. «Лаборатория Касперского»: *«DDoS-атака — это только следствие, верный признак того, что у вашей организации есть недоброжелатели. Для обеспечения безопасности нужно бороться с причиной нападения.».*

Основной целью DDoS-атаки является нарушить непрерывность бизнес-процессов компании тем самым нанеся финансовый и репутационный ущерб жертве. Атаки в основном направлены на веб-ресурсы в 90% случаях на формы авторизации в сервисах.

Помимо использования «botnets» DDoS-атаку можно выполнить, зная уязвимости в веб-сервисе жертвы. Зная уязвимость, злоумышленник может написать вредоносное ПО, эксплуатирующее данную уязвимость. Поэтому важно своевременно выявлять и устранять данные уязвимости в веб-сервисах. В данной работе будут рассмотрены новейшие меры защиты от DDoS-атак. А также методы обнаружения уязвимостей в веб-сервисах связанных с DDoS.

Основная часть. 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.

Response Rate Limiting

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. Однако следует помнить, что не всегда владельцы DNS-серверов готовы прибегать к использованию таких механизмов. Ведение базы адресов требует определенных ресурсов. Кроме того, не всегда владельцы таких серверов обеспокоены тем, что их серверы используются для осуществления атак, а также не всегда замечают увеличение нагрузки на сервер в периоды их использования для реализации атак.

Defense By Offense

Есть интересное предложение, опубликованное Walfish et. Al [26] в котором рассматривается защитная мера от DDoS-атаки на уровне приложений. Предлагается отправка большего объема трафика [26]. Логика этой схемы не в том, чтобы просто замедлить плохих клиентов, но поощрение хороших клиентов для отправки большего объема трафика. Это предполагает, что, если плохие клиенты уже используют большую часть их загрузки, поощряя клиенты, отправляющие больший объем трафика, будут изменение только количества хороших клиентов. Здесь плохие клиенты занимают более высокую долю пропускная способность. Имея схему оповещения, пропускная способность теперь больше занята хорошим клиентов. Атакованный сервер с функцией Speak-up ему нужен механизм для измерения пропускной способности. Его основная обязанность – увеличивать пропускную способность для хороших клиентов. И уменеьшать для плохих.

Активная Фильтрация, Ip Traceback

Проделана значительная работа по защите жертвы DDoS-атак за счет методы активной фильтрации [16]. Данная архитектура защиты создана на основе шлюза. Данная архитектура описывается в статье от Xuan et. al. [16]. Это предлагает систему защиты для обнаружения атак и способы их контроля. Защищает TCP дружественный трафик, занимающий основную часть пропускной способности сервера. Шлюзы развернуты в разных места в сети для обнаружения атак и также выполняют контроль доступа к трафику.

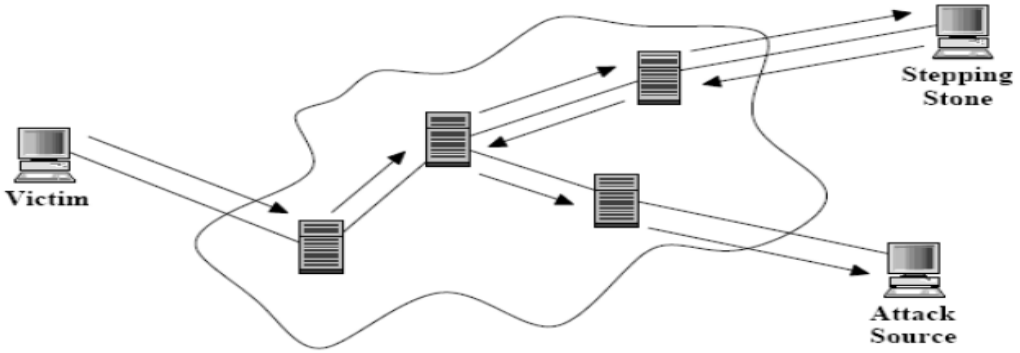

Рисунок 2. Trace across a Stepping Stone

В другой работе Yaar et. Al [16]. предложил новую идею, где предложил маркировку пакетов на основе схемы Pi, а также новый тип механизмов фильтрации [20]. Схема защиты Pi от DDoS-атак состоит из алгоритма маркировки пакетов, который кодирует полный Pi в каждом пакете. Это также состоит из алгоритма фильтрации пакетов, который определяет, на сколько эффективно жертва DDoS-атаки использует эту схему. По методу IP-трассировки есть отличная работа Strayer et. Al [7]. В данной работе предлагается архитектура многоэтапного отслеживания для защиты от DDoS-атак. Эта архитектура называется Stealthy Tracing. Attackers Research Light TracE (STARLITE), которая является расширенной версией Source Path Изолирующий движок (SPIE) [30]. Это STARLITE архитектура создает прототип для интеграции прослеживание одного пакета со ступенькой обнаружение. Чтобы проследить путь атаки через хосты отмывания, которые также называют ступеньками в этом контексте цепочка соединения. Цепочка связей между злоумышленником и жертвой. Архитектура SPIE базовая архитектура SPIE система. SPIE — это трассировка на основе журнала система. Основы трассировки IP-пакетов зависят от аудита сетевых маршрутизаторов. Прослеживание SPIE Менеджер (STM) отвечает за контроль над всей системой. Система STARLITE объединяет концепция обнаружения ступеней в SPIE системах для использования разнообразных коммуникаций инфраструктуры SPIE. Многоступенчатая трассировка - шаг 1, предлагаемая в STARLITE многоступенчатая трассировка: показано на рисунке 3.

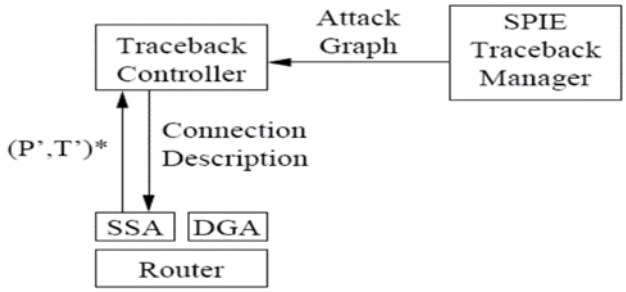

Рисунок 3. Многоступенчатая трассировка шаг 1.

Здесь P обозначает пакет, V - жертва, а T - время атаки. DGA - агенты генерации данных. SSA расшифровывается как Stepping Stones Aggregator. Многоступенчатая трассировка - Шаг 2. Он показывает, как Traceback Контроллер (TBC) получает график атак, идентифицирует маршрутизатор и, наконец, извлекает описание соединения из

отслеживаемого пакета. Обратная связь Контроллер возвращается к отслеживанию SPIE Менеджер просить SPIE о строительстве нового запрос на основе пакета из входящего подключение, а затем продолжить трассировку.

Сканер уязвимостей

Уязвимость — это недостаток или слабость приложения, которое может быть недостатком дизайна или ошибкой реализации, что позволяет злоумышленнику наносить вред заинтересованным сторонам приложения [10]. Заинтересованные стороны включают владельца приложения, пользователей приложений и другие объекты [9]. Эта технологическая структура была выбрана из-за ее популярности и широкого использования. Каждый сканер уязвимостей веб-приложений протестирован против веб-приложения по предписанному подходу, который включает в себя набор процедур инициализации, выполнения, классификации и анализа. Используя безопасную и небезопасную версию настраиваемого веб-приложения, ложноположительные и ложноотрицательные результаты могут быть связаны с методами, используемыми сканерами для обнаружения уязвимостей. Эта связь между используемыми методами и ложноположительными или ложными негативами может быть использована, чтобы предложить улучшения для методов сканирования веб-приложений [11]. Шаг 1. Ввод URL-адреса. Шаг 2. Выбор типа уязвимости, которую необходимо отсканировать. Шаг 3. Запуск сканирования. Шаг 4: Проверка данных условий в соответствии с выбранным сканированием уязвимостей. Шаг 5: После наблюдения за условиями выбранной уязвимости выводится отчет.

На основе общего алгоритма разработаны конкретные алгоритмы для обнаружения определенных уязвимостей, благодаря которым можно произвести DoS – атаку.

Выводы. Растущее число 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. В том числе планируется проведение экспериментов по оценке эффективности методов защиты от DNS-атак, модифицированных для работы с другими протоколами, используемыми для реализации атак, основанных на отражении трафика. Полученные результаты будут учитываться при разработке новых методов защиты от атак, в основе которых лежат механизмы отражения и усиления вредоносного трафика.

References

1. Dong Xuan, Riccardo Bettati, and Wei Zhao; A Gateway-based Defense System for Distributed DoS Attacks in High-Speed Networks; 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June 2001; pp. 212-219.

2. Yu Chen, Kai Hwang, and Yu-Kwong Kwok; Filtering of Shrew DDoS Attacks in Frequency Domain; Proceedings of The 7th World Multiconference on Systemics, Cybernetics and Informatics (SCI 2003), Orlando, Fl, July 2003.

3. Abraham Yaar, Adrian Perrig, Dawn Song; StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense; IEEE Journal, Vol.

4, Issue 10, Oct. 2006; pp.1853 – 1863 19. Yu Chen; Kai Hwang; Yu-Kwong Kwok; Filtering of shrew DDoS attacks in frequency domain; Local Computer Networks, 2005. IEEE Conference on 15-17 Nov. 2005; Page(s):8 pp.

5. Paul J. Criscuolo; Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, And Stacheldraht CIAC-2319; Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev.1, Lawrence Livermore National Laboratory, February 14, 2000.

6. Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger, Scott Shenker; DDoS Defence by Offense; ACM SIGCOMM'06, Pisa, Italy; September 11-15, 2006.

7. Tim Strayer, Christine Jones, Beverly Schwartz, Joanne Mikkelson, Carl Livadas; Architecture for multi-stage network attack traceback; Proceedings of the IEEE LCN Workshop on Network Security (WoNS'2005); Sydney Australia; 15-17 November 2005; pp. 8.

8. A.C. Snoeren, C. Partridge, L.A. Sanchez, C.E. Jones, F. Tchakountio, B. Schwartz, S.T. Kent, W.T. Strayer; Single-Packet IP Traceback; ACM/IEEE Transactions on Networks, December 2002.

9. Qunfeng Dong, Suman Banerjee, Micah Adler, Kazu Hirata; Efficient Probabilistic Packet Marking; ICNP 2005; 6-9 Nov 2005; pp. 10.

10. Xiaowei Yang, David Wetherall, Thomas Anderson; A DoS-limiting Network Architecture; Proceedings of ACM SIGCOMM 2005; Vol.35, No.4, August 2005; pp. 241-252.

11. Lin Cai, Jianping Pan, Shen S.X; Vulnerability analysis of IP traceback schemes; Global Telecommunications Conference 2005, IEEE; Vol.3, 28 Nov-2 Dec 2005; pp. 5.