АВТОМАТИЗИРОВАННЫЙ ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ФИЛЬТРАЦИИ СЕТЕВОГО ТРАФИКА ПРИ РАСПРЕДЕЛЕННЫХ АТАКАХ НА ОТКАЗ В ОБСЛУЖИВАНИИ

Дмитриев А.А., Гладнев А.С.
Алтайский государственный университет, г. Барнаул
email: dmitriev@asu.ru

Аннотация. Предложено программное обеспечение, позволяющее блокировать сетевой трафик с выделенных устройств, участвующих в распределенной сетевой атаке. Фильтрация сетевого трафика осуществляется на граничном маршрутизаторе с помощью списка блокирующих правил. Для составления надежного фильтрующего списка проведен анализ сетевого трафика. Показано, что при выполнении блокировки достаточно использовать сетевые адреса атакующих устройств. Работа программного комплекса апробирована на сетевом оборудовании компании Cisco. Полученные результаты могут быть использованы для создания новых технических средств смягчения распределенной атаки на сетевые ресурсы организаций.

Ключевые слова: распределенная атака, фильтрация сетевого трафика, анализ трафика.

Введение

Распределенные сетевые атаки типа «Отказ в обслуживании» являются одним из распространённых способов воздействия на сетевую инфраструктуру организаций с целью отказа в работе вычислительной сети [1, 2]. Реализация атаки сводится к одномоментной отправки с устройств злоумышленника множества сетевых пакетов, которые по каналам связи доставляются в локальную сеть организации. В виду технического сходства создаваемого злоумышленником трафика с обычными сетевыми пакетами, передающими полезные данные пользователей, устройства в локальной сети стремятся обработать нежелательный трафик, что приводит к их перегрузке и отказу в работе [3, 4]. Способность организации к сопротивлению распределенной атаке зависит, прежде всего, от принимаемых технических контрмер. Подобные контрмеры включают установку на границе сети мощного фильтрующего трафик оборудования. В качестве такого оборудования выступают межсетевые экраны (файерволы), обладающие необходимым программным функционалом для фильтрации трафика и ограничения скорости передачи нежелательных данных в момент проведения атаки [5]. Стоит отметить, что многие современные файерволы зачастую имеют возможность подключения к специальным базам данных, содержащим информацию об зараженных устройствах в сети Интернет. В момент проведения распределенной атаки информация об ip-адресах устройств, помещенных в базу данных, применяется для создания актуальных фильтрующих правил, блокирующих передачу данных от зараженных устройств в локальную сеть организации. Несмотря на перечисленные функциональные преимущества, файерволы, особенно в программно-аппаратном исполнении, являются достаточно дорогими устройствами для использования в сетях маленьких организаций.

Другим методом смягчения распределенной атаки является перенаправление потока трафика, предназначенного атакуемым устройствам, в сеть сторонней организации, обладающей необходимыми аппаратными ресурсами для фильтрации [6]. Перенаправление сетевого трафика осуществляется при помощи системы доменных имен [2]. Проводится изменение с целью преобразования доменных имен атакуемых устройств в ip-адреса внешней организации. Таким образом, поток

трафика при распределенной атаке отправляется в стороннюю сеть, в которой фильтруется при помощи ее программно-аппаратных ресурсов. После обработки полезная часть сетевого трафика возвращается в сеть атакуемой организации. Применение данного способа защиты от распределенных атак, возможно, только после времени, необходимого для обновления информации в системе доменных имен об новых ip-адресах устройств атакуемой организации.

В целом для успешного применения перечисленных мер противодействия распределенной атаки требуются добавление в локальную сеть организации межсетевого экрана, а также правильной технической настройки соответствующего оборудования для перенаправления трафика. С другой стороны, при создании локальной сети в ее состав включают маршрутизатор, который является граничным устройством, соединяющим локальную сеть организации и сеть Интернет [7]. Маршрутизатор используется для пересылки трафика между отдельными сетями, а его программное обеспечение, позволяет реализовать набор фильтрующих правил, блокирующих передачу нежелательных данных из сети Интернет. В настоящей работе разработано программное обеспечение, реализующее алгоритм автоматического создания фильтрующего списка правил на маршрутизаторе для предотвращения распределенной атаки.

Формирование списка правил

При создании списка фильтрующих правил для маршрутизатора в работе использовался следующий подход, по которому блокирование нежелательного трафика производилось по сетевым адресам конечных узлов, задействованных в распределенной атаке. По своей структуре список фильтрации состоял из набора блокирующих правил, запрещающих передачу данных с отдельных ip-адресов сети Интернет [8, 9]. Затем в конце списка блокирующих правил применялось разрешающее правило для передачи полезного сетевого трафика, предназначенного пользователям сети. Для уменьшения количества запрещающих правил ip-адреса атакующих устройств были объединены в укрупненные логические подсети с более широкой десятичной маской [7].

В созданном списке правил фильтрация пакетов проводилась только по протоколу ip. Применение правил фильтрации с использованием дополнительных параметров портов источника и назначения протоколов транспортного уровня tcp или udp без указания сетевых адресов источника трафика в большинстве случае неоправданно и приводит к фильтрации полезного трафика [5]. Во время атаки вместе с полезным трафиком нежелательные пакеты данных передаются между устройствами в направлении из сети Интернет в локальную сеть организации. При формировании пакетов для отправки в атакуемую сеть порт источника в большинстве случаев выбирается атакующими сетевыми устройствами случайным образом. Порт назначения задается из диапазона общеизвестных портов, которые связанны с популярными приложениями, например, http или https. Сделанные выводы подтверждают результаты анализа сетевого трафика, записанного при распределенной атаке на веб-ресурсы сети Алтайского государственного университета[1]. На рис. 1 в виде гистограммы показано количество пакетов, переданных в сеть организации с помощью протокола tcp в первые минуты проведения атаки [10].

[1] Дистант - это новые возможности. Алтайский госуниверситет перестроил учебный процесс. Российская газета. [Электронный ресурс]. // Режим доступа: https://rg.ru/2020/04/30/reg-sibfo/altajskij-gosuniversitet-perestroil-uchebnyj-process.html – Загл. с экрана. Дата обращения: 02.11.2020.

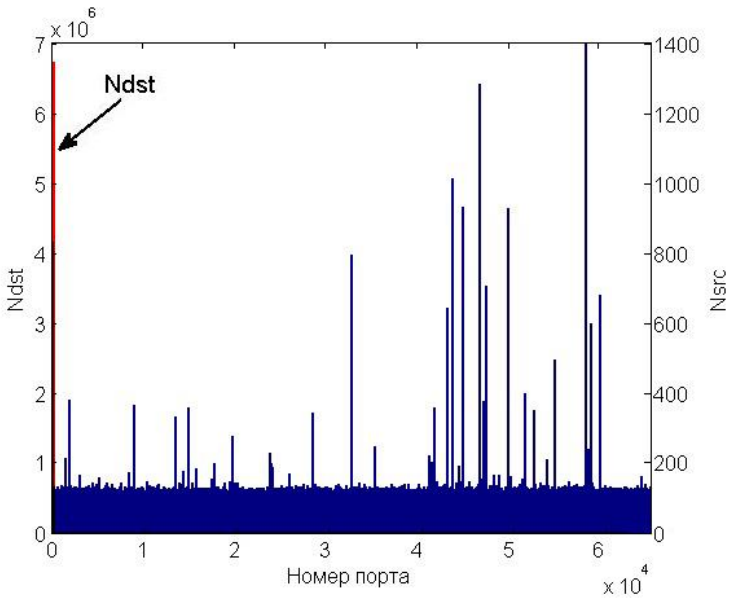

Рисунок 1. Распределение исследованных сетевых пакетов по номерам портов.

На рис. 1 на графике Ndst – Номер порта присутствует выраженный одиночный пик, который соответствует числу пакетов с одним уникальным портом назначения. Одиночный пик гистограммы свидетельствует о том, что основное число сетевых пакетов были переданы преимущественно на порт веб-сервера организации, подвергнутый сетевой атаке. Отметим, что в данный пик описывает, в том числе, пакеты, отправленные в сеть для получения обычных данных с сервера. Столбцы графика Nsrc – Номер порта иллюстрируют количество пакетов с различными номерами портов источников в записанном трафике. Наблюдаемые пики гистограммы распределены вдоль всего диапазона возможных портов, что указывает на случайный характер их выбора при отправке пакета. Таким образом, применение фильтрации по группе портов источников либо по отдельному порту назначения без указания ip-адреса источника в этом случае приведет к блокированию части полезного трафика, передаваемого в локальную сеть организации.

Программное обеспечение для смягчения распределенных атак

Для защиты локальной сети в момент проведения сетевой атаки в работе разработано программное обеспечение для маршрутизаторов компании Cisco серии 2900 [9]. Схема работы программного обеспечения показана на рис. 2.

Согласно представленному алгоритму из рис. 2 на первом этапе работы программа формировала список ip-адресов устройств, с которых происходила сетевая атака. Список ip-адресов составлялся автоматически программным обеспечением с помощью подключения к внешним базам данных организаций, занимающихся мониторингом устройств, задействованных в распределенных атаках. Полученные адреса группировались и объединялись в отдельные укрупненные подсети. Затем создавался набор фильтрующих правил с указанием отдельных ip-адресов или созданных подсетей. Объединение сетевых адресов в укрупненные подсети позволило снизить нагрузку на маршрутизатор на этапе непосредственной фильтрации трафика. Полученный после объединения список ip-адресов имел меньшее число записей, и, следовательно, уменьшалось затрачиваемое время при последовательном поиске ip-адреса атакующего устройства. Полученный список правил применялся к порту маршрутизатора, подключенному к сети Интернет. После создания списка правил и его применения на интерфейсе маршрутизатора выполнялась фильтрация входящего в локальную сеть организации сетевого трафика. Надежность блокировки сетевого трафика обеспечивалась операционной системой маршрутизатора.

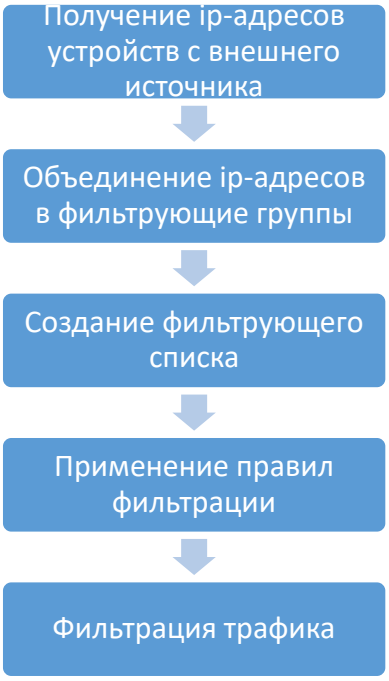

Рисунок 2. Алгоритм работы программного обеспечения.

Выводы

В работе описан подход к разработке программного обеспечения для защиты локальной сети организации от распределенной атаки, приводящей к отказу в обслуживании сетевого оборудования. В локальных сетях организаций для обеспечения подключения к внешним сетям используется маршрутизатор, который применяется для фильтрации пакетов сетевых данных. Реализованное в работе программное обеспечение, выполняемое на маршрутизаторе, автоматически формирует набор фильтрующих правил препятствующих пересылки пакетов со стороны внешних устройств, участвующих в распределенной атаке. Применение программного обеспечения на практике может использоваться в качестве одной из технических контрмер для смягчения распределенной сетевой атаки на ресурсы локальной сети организации.

Библиографический список

1. Garber L. Denial-of-Service Attacks Rip the Internet // IEEE Computer. – 2000. – Vol. 33. - Iss. 4. – pp. 12–17.
2. Бирюков А.А. Информационная безопасность: защита и нападение // М.: ДМК Пресс, 2012. – 474 с.
3. Lu W., Traore I. An unsupervised approach for detecting DDoS attacks based on traffic-based metrics // IEEE Pacific Rim Conference on Communications, Computers and signal Processing PACRIM 2005. 24–26 Aug. 2005. - pp. 462–465.
4. Noh S., Lee C., Choi K., Jung G. Detecting distributed denial of service (DDoS) attacks through inductive learning // Lecture Notes in Computer Science. Berlin, Springer. – 2003. - Vol. 2690. - pp. 286-295.
5. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях // М.: ИНФРА-М. - 2011. – 416 с.
6. Mahajan D. DDoS Attack Prevention and Mitigation Techniques - A Review // International Journal of Computer Applications. – 2013. – Vol. 67. – Iss. 19. – pp. 21–24.

7. Кузьменко, Н.Г. Компьютерные сети и сетевые технологии // СПб.: Наука и техника, 2013. – 368 с.
8. Teare D., Vachon B., Graziani R. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide // Indianapolis: Cisco Press, 2015. – 726.
9. Амато В. Основы организации сетей Cisco. // М.: Издательский дом "Вильямс", 2002. – 512 с.
10. Зрелов П.В., Иванов Вал.В., Иванов Вик.В., Крюков Ю.А., Татаринов И.И. Исследование особенностей Интернет-трафика в магистральном канале // Письма в ЭЧАЯ. – 2019. – Т. 16. - №3 (222). – С. 261 – 276.

SOFTWARE FOR NETWORK TRAFFIC FILTERING DURING DISTRIBUTED DENY OF SERVICE ATTACKS

Dmitriev A.A., Gladnev A.S.
Altai State University, Barnaul
email: dmitriev@asu.ru

Abstract. In present paper software is proposed that allows blocking network traffic from dedicated devices involved in a distributed network attack. Network traffic is filtered on the border router using a list of blocking rules. Network traffic analysis is used for compile a reliable filtering list. It is shown that network addresses of attacking devices are used to reliably block unwanted traffic. Software has been tested on Cisco network routers. Obtained results can be used to create new technical means of mitigating a distributed attack on the network resources of organizations.

Key words: distributed attack, network traffic filtering, traffic analysis.