УДК 004.056.57

МЕТОД ФИЛЬТРАЦИИ ТРАФИКА НА ОСНОВЕ АНАЛИЗА СЕТЕВЫХ ВЗАИМОДЕЙСТВИЙ УСТРОЙСТВ

Дмитриев Александр Александрович, Дмитриев Денис Александрович

Алтайский государственный университет, г. Барнаул
e-mail: dmitriev@asu.ru

TRAFFIC FILTERING METHOD BASED ON ANALYSIS OF NETWORK INTERACTIONS OF DEVICES

Dmitriev Alexander A., Dmitriev Denis A.

Altai State University, Barnaul

Аннотация. В работе предложен метод защиты сетевой инфраструктуры организации на основе анализа сетевой активности взаимодействующих устройств. Показано, что заражение устройств пользователей может привести к отсылке множества сетевых запросов к другим устройствам в сети. Для выявления подобной сетевой активности компьютеров в работе использованы данные о сетевых взаимодействиях, полученные при помощи протокола Netflow. С помощью подсчета числа активных соединений определены сетевые адреса зараженных устройств. Для осуществления быстрой блокировки зараженных компьютеров в работе реализована передача данных о сетевых адресах на межсетевой экран. Применение предложенного метода защиты позволило улучшить контроль сетевых взаимодействий между устройствами и защиту локальной сети.

Ключевые слова: вредоносное программное обеспечение, защита локальной сети, межсетевой экран.

Abstract. The paper proposes a method for protecting an organization's network infrastructure based on an analysis of the network activity of interacting devices. It has been shown that infection of user devices can lead to multiple network requests being sent to other devices on the network. To identify such network activity of computers, the work used data on network interactions obtained using the Netflow protocol. By counting the number of active connections, the network addresses of infected devices are determined. To quickly block infected computers, the work implements the transfer of data about network addresses to the firewall. The use of the proposed protection method made it possible to improve the control of network interactions between devices and the protection of the local network.

Keywords: malicious software, local network protection, firewall.

Для цитирования: Дмитриев А.А., Дмитриев Д.А. Метод фильтрации трафика на основе анализа сетевых взаимодействий устройств // Проблемы правовой и технической защиты информации. 2023. №11. С. 16-20.

For citation: Dmitriev A.A., Dmitriev D.A Traffic filtering method based on analysis of network interactions of devices // Legal and Technical Problems Information Protection. 2023. No. 11. P. 16-20.

Введение. Обеспечение защиты от воздействия вредоносного программного обеспечения на сетевую инфраструктуру организаций является сегодня актуальной задачей для специалистов в области информационной безопасности и сетевых

инженеров [1-3]. Обычно комплекс мероприятий для защиты сетевых устройств включает установку антивирусных программ и своевременное обновление используемых в организации операционных систем и пользовательских программ [4-5]. Однако работа нового вредоносного программного обеспечения, характеристики и действия которого еще не изучены, может быть не определена антивирусными системами. В связи с этим в последнее время для защиты локальных сетей все чаще используют системы мониторинга и контроля сетевой активности устройств [6-7]. Эти системы позволяют выявить аномалии в сетевом трафике взаимодействующих устройств, связанные с действием вредоносных программ, что позволяет оперативно заблокировать зараженные устройства пользователей.

В настоящей работе предложен новый подход к защите сетевой инфраструктуры организации на основе идентификации зараженных устройств с помощью анализа сетевых соединений.

Описание топологии локальной сети. В настоящей работе использована локальная сеть организации, топология которой представлена на рис. 1.

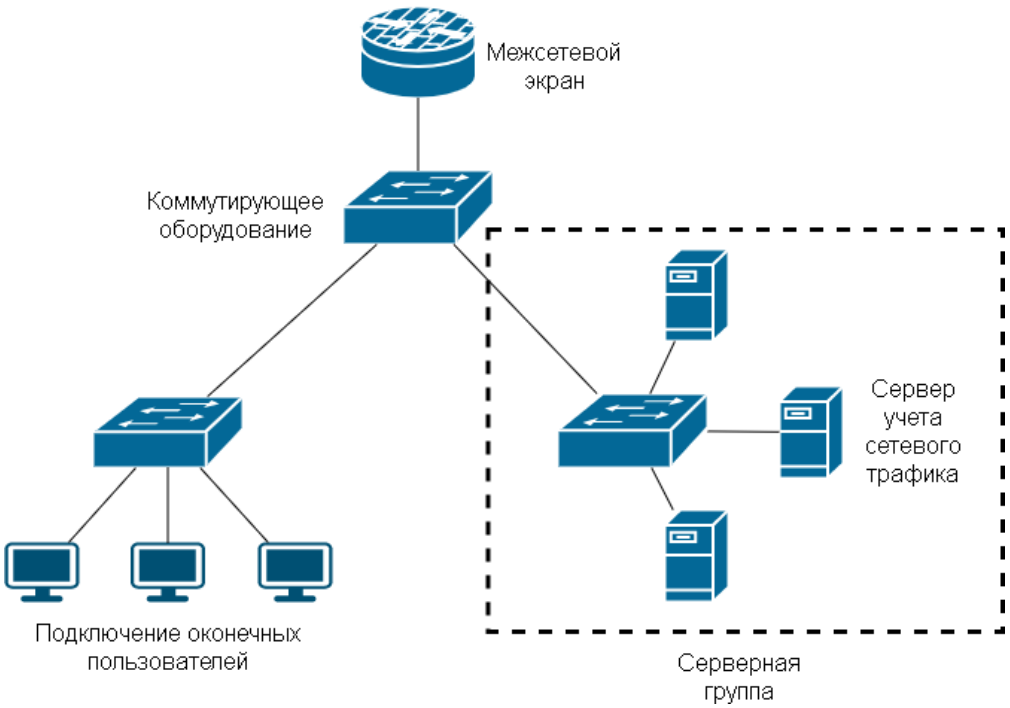

Рисунок 1. Схема локальной сети, используемая для изучения сетевой активности устройств пользователей

Согласно рис. 1, в качестве основы для построения локальной сети в организации использовалась топология типа «Звезда» [8]. Коммутаторы производителей Elteh MES2324P и Cisco Catalyst 2960 применялись для подключения устройств пользователей, серверной группы и межсетевого экрана. Серверная группа состояла из аппаратных серверов, обеспечивающих работу различных информационных и служебных сервисов организации. На отдельных серверах работали сетевые веб-службы, система управления базой данных MySQL для обработки персональных данных сотрудников. Также в серверную группу был включен отдельный сервер для мониторинга оборудования и учета сетевого трафика. Устройства пользователей и сервера из серверной группы были разделены в две различные логические подсети. Каждая подсеть имела отдельный номер виртуальной локальной сети (влан). Вланы терминировались на межсетевом

экране Usergate. Межсетевой экран Usergate применялся для маршрутизации сетевого трафика между подсетями и доступа пользователей в сеть Интернет. Защита сети организации от внешних атак и фильтрация сетевого трафика обеспечивалась внутренним программным обеспечением файервола Usergate [9].

Реализация системы фильтрации. Для реализации защиты локальной сети при действии зловредного программного обеспечения в работе был применен подход, включающий одновременную работу сервиса учета сетевого трафика и аппаратного межсетевого экрана. Сервис учета сетевого трафика в настоящей работе был реализован на основе программного обеспечения, собирающего данные о сетевых взаимодействиях устройств при помощи протокола Netflow [9]. Для этого на отдельном аппаратном сервере под управлением операционной системы Debian было установлено программное обеспечение протокола Netflow. При помощи протокола Netflow собирались данные об межсетевых взаимодействиях устройств с межсетевого экрана (рис. 1). При передаче данных между устройствами в памяти файервола сохранялись данные о сетевых параметрах соединений. Затем эти данные передавались с файервола на созданный сервер учета сетевого трафика. На сервере с помощью установленного программного обеспечения из полученных данных выделялись следующие параметры: ip-адресация взаимодействующих устройств, используемый транспортный протокол, номера портов и количество переданных байт между устройствами. Выделенные параметры сетевого соединения сохранялась в базе данных PostgreSQL для оперативного доступа с целью последующей обработки для определения устройств, с которых наблюдалась вредоносная активность.

Обработка сохраненных данных проводилась для определения ip-адресов устройств, которые наиболее активно передавали сетевой трафик и имели большое количество одномоментных сетевых соединений с другими устройствами. Для этого из базы данных PostgreSQL выбиралась информация о параметрах сохраненных сетевых соединений, произведенных в течение предшествующих 60 секунд от текущего времени. Из полученных записей выделялись ip-адреса устройств, если выполнялись следующие условия. Для конкретного ip-адреса, закрепленного за сетевым устройством, наблюдалось более десяти сетевых соединений с другими устройствами, и происходила передача меньше 100000 байт данных. Представленные здесь триггерные значения числа соединений и количества переданных байт данных для идентификации ip-адреса в настоящей работе подобраны экспериментально для представленной локальной сети и могут быть адаптированы для других сетей различной сложности и конфигурации. Так как создание большого числа одномоментных соединений, в которых передается малое количество байт полезной информации, является типичным обменом данных в случае действия зловредного программного обеспечения, то в данной работе считалось, что определенные через ip-адреса устройства являлись источниками при проведении атак. Поэтому в дальнейшем выделенные ip-адреса устройств подвергались фильтрации с помощью межсетевого экрана.

Для обеспечения фильтрации сетевых пакетов на межсетевом экране Usergate было создано специальное правило, позволяющие блокировать сетевой трафик при передаче между устройствами в компьютерной сети. Особенностью созданного правила фильтрации являлось наличие в нем специального списка ip-адресов, в который добавлялись ip-адреса, выделенные после обработки сетевых данных на сервисе учета сетевого трафика. Для быстрого обновления списка в работе был использован внутренний функционал межсетевого экрана Usergate, позволяющий добавлять ip-адреса в блокирующий список из специального файла, размещенного на отдельном веб-сервере, как показано на рис. 2.

На сервисе учета сетевого трафика было установлено программное обеспечение для работы веб-сервера Apache [10]. Выбор в пользу программного обеспечения Apache был обусловлен простотой установки и настройки этого веб-сервера, а также широким применением этого программного обеспечения в компьютерных сетях для безопасного размещения различных сайтов. На настроенном веб-сервере были созданы два текстовых файла. Первый текстовый файл содержал ip-адреса устройств, подлежащих фильтрации, а второй текстовый файл содержал номер обновления текущего списка. Номер обновления списка автоматически увеличивался при добавлении или удалении ip-адресов атакующих устройств в первый текстовый файл. Для быстрой загрузки файла с ip-адресами на межсетевой экран этот текстовый файл был предварительно упакован в архив. Инициатором загрузки заархивированного файла с ip-адресами являлся межсетевой экран, который контролировал изменения номера обновления во-втором файле. При увеличении номера обновления межсетевой экран скачивал архив и размещал ip-адреса из файла в список в правиле фильтрации. Таким образом, обеспечивалась фильтрация сетевого трафика по определенным ip-адресам на межсетевом экране.

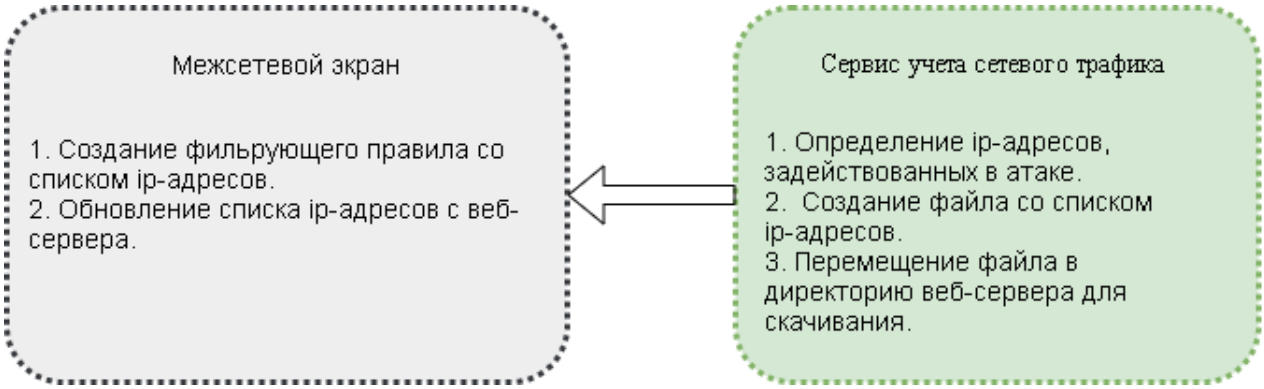

Рисунок 2. Схема взаимодействия между межсетевым экраном и сервисом учета сетевого трафика

Вывод. Создание новых подходов к защите сетевой инфраструктуры позволяет уменьшить потенциально опасное воздействие вредоносных программ на сетевое оборудование и компьютеры пользователей. В работе рассмотрен метод защиты локальной сети организации на основе выявления аномалий в сетевой активности устройств, обусловленных множественными исходящими сетевыми запросами. Предложенный метод использует распространенное программное обеспечение протокола Netflow для получения данных о взаимодействующих по сети устройствах. Выявление подозрительной активности построено на подсчете суммарного числа запросов от сетевого устройства в течение заданного периода времени. Для блокировки зараженных устройств использован внутренний программный функционал межсетевого экрана Usergate. Предложенный метод защиты может быть использован для повышения уровня защищенности локальных сетей организаций.

Библиографический список

1. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2012. – 474 с.

2. Mahajan D. DDoS Attack Prevention and Mitigation Techniques - A Review // International

Journal of Computer Applications. – 2013. – Vol. 67, Iss. 19. – Pp. 21–24.

3. Ширяев, А.В. Некоторые способы совершения компьютерных преступлений в сети Интернет / А.В. Ширяев, В.В. Поляков // Проблемы правовой и технической защиты информации. - 2018. –No6 - С. 156-161.

4. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: ИНФРА-М, 2011. – 416 с.

5. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М.: Стандартинформ, 2018. – 16 с.

6. Васильков А.В. Информационные системы и их безопасность: учеб, пособие / А. В. Васильков, А. А. Васильков, И. А. Васильков. – М: Форум, 2011. – 527 с.

7. Минакова Н.Н. Методы и средства защиты информации в коммерческой организации / Минакова Н.Н., Поляков В.В., Плетнев П.В. Барнаул: Изд-во «Новый формат», 2016. – 158 с.

8. Кузьменко, Н.Г. Компьютерные сети и сетевые технологии. – СПб.: Наука и техника, 2013. – 368 с

9. Конахович, Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов. – К.:"МК-Пресс", 2005. — 288 с.

10. Арнольд, М. Администрирование APACHE / М. Арнольд, Дж. Алмейда, К. Миллер. – Издательство: Лори. – 2021. – 418 с.