Список використаних джерел:

1. P. Viola and M. J. Jones, «Rapid Object Detection using a Boosted Cascade of Simple Features», proceedings IEEE Conf. on Computer Vision and Pattern Recognition (CVPR2001), 2001 (Kauai, HI, 2001), pp. 511–518.

2. Viola P., Jones M. J. Robust real-time face detection. *International Journal of Computer Vision.* Vol. 57, no. 2, 2004. P. 137–154

3. Азаров Д. Метод распознавания лиц Виолы-Джонса (Viola-Jones) https://oxozle.com/2015/04/11/metod-raspoznavaniya-lic-violy-dzhonsa-viola-jones/

4. Метод Виолы-Джонса (Viola-Jones) как основа для распознавания лиц https://habr.com/ru/post/133826/

5. Кардаш А. І., Левицька С. М., Дудикевич А. Т. Задача розпізнавання людських облич методами штучного інтелекту. *Інформаційні технології та комп'ютерна інженерія.* 2013, № 1. С. 84–87.

Ключові слова: розпізнавання облич, метод Віоли-Джонса, інтегральне подання зображень, ознаки Хаара.

Key words: face recognition, Viola – Jones method, integral representation of images, Haar features.

Ключевые слова: распознавание лиц, метод Виолы-Джонса, интегральное проедставление изображений, признаки Хаара.

***Науковий керівник**: к.т.н., доц. Трофименко О. Г.*

Павловский Владислав Юрьевич
Национальный университет «Одесская юридическая академия»,
студент 4-го курса факультета кибербезопасности
и информационных технологий

ЗАЩИТА ОТ DDOS-АТАК

Распределенные атаки типа «отказ в обслуживании» (Распределенный отказ в обслуживании или DDoS) сегодня часты, в частности, из-за относительной простоты их реализации и их эффективности против неподготовленной цели.

Эти атаки могут привести к значительным финансовым потерям из-за прерывания обслуживания или даже косвенно через повреждение имиджа цели. По этой причине необходимо предвидеть эту угрозу и принять ряд технических и организационных мер, чтобы противостоять ей.

Атака отказа в обслуживании направлена на то, чтобы сделать одну или несколько служб недоступными. Отказ в обслуживании может заключаться в использовании, например, уязвимости программного или аппаратного обеспечения. Прерывание обслуживания также может быть выполнено путем предотвращения доступа к этой услуге, например, путем насыщения полосы пропускания сети: это называется объемными атаками. Кроме того, атака может запрашивать до исчерпания один или несколько ресурсов службы. Это может быть, например, открытие большого количества новых сеансов TCP за очень короткий промежуток времени или даже слишком большое количество одновременных обработок, выполняемых базой данных [1].

Любая организация, деятельность которой зависит от сетевой инфраструктуры, подключенной к Интернету, может стать целью DDoS-атаки. Мотивы и цели нападавших разнообразны: от идеологических претензий до мести, включая вымогательство. Более того, некоторые атаки, похоже, проводятся для того, чтобы отвлечь внимание и скрыть другие незаконные действия, такие как мошеннические банковские операции. Хотя многие организации подвержены этой угрозе, некоторые виды деятельности более подвержены атакам DDoS. Среди них, в частности, можно упомянуть электронную коммерцию финансовых учреждений, правительства или даже ИТ-хостинговые структуры. В этом контексте тем более важно предоставить соответствующие решения защиты с самого начала проектов по настройке информационных систем и сетевой инфраструктуры.

Существуют различные защитные решения, которые могут быть реализованы для борьбы с DDoS-атаками. Развертывание

фильтрующего оборудования на границе информационной системы объекта обеспечивает защиту от атак, объем которых не превышает пропускную способность сетевых каналов. Когда сетевые каналы организации перегружены, часто необходимо обратиться к транзитному оператору или поставщику Интернет-услуг, чтобы отфильтровать восходящий трафик. Кроме того, поставщики услуг предлагают специальные решения для защиты под названием «в облако», которые размещаются на собственной инфраструктуре. Можно совместить использование выделенного оборудования на границе сети объекта с фильтрацией, выполняемой «в облако». Этот тип гибридной защиты позволяет, в частности, защитить объект от объемных атак, давая ему возможность бороться с атаками с низкой пропускной способностью [4].

Оборудование типа межсетевого экрана. Брандмауэры и балансировщики нагрузки могут помочь отразить некоторые DDoS-атаки, например, с относительно низким трафиком. Таким образом, брандмауэры можно использовать для фильтрации трафика в соответствии с транспортным протоколом и портами источника или назначения или даже для ограничения количества запросов на исходный IP-адрес к серверу. Действительно, некоторые DDoS-атаки специально направлены на исчерпание ресурсов памяти цели. В этом случае брандмауэры и балансировщики нагрузки являются первыми элементами инфраструктуры, которые будут затронуты. Поскольку эти элементы отключены, отказ одного из них достаточен, чтобы отказ в обслуживании стал эффективным. Однако иногда можно изменить конфигурацию этого оборудования, чтобы повысить его устойчивость к атакам этого типа, например, увеличив размер таблиц состояния и сократив время мониторинга соединения.

Использование специального оборудования. Организация может использовать оборудование для фильтрации, специфичное для DDoS-атак. Это оборудование обычно имеет подходящую производительность и предлагает несколько типов

противодействия. Помимо функций фильтрации по белому или черному списку, они позволяют, среди прочего:

– проводить фильтрацию по географическому положению источников;

– определять точные правила фильтрации пакетов по их содержимому (например, используя регулярные выражения);

– ограничить количество запросов в заданном временном интервале для определенных ресурсов (например, для веб-страницы)

– определить пороги обнаружения атак в соответствии с такими параметрами, как пропускная способность или количество пакетов в секунду.

Следует также отметить, что этот тип оборудования может использоваться для фильтрации приложений, когда обмены зашифрованы (например, для трафика HTTPS), позволяя объекту сохранять свой закрытый ключ [5].

Фильтрация на уровне сети транзитного оператора. Транзитный оператор может настроить фильтрацию трафика на основе IP-адресов источника или назначения, используемого транспортного протокола, а также портов источника или назначения. Следует отметить, что фильтрация исходных IP-адресов может быть затруднена, если их очень много. В крайнем случае оператор может исключить весь трафик в заданный пункт назначения. В этом случае трафик к одному или нескольким получателям просто не обрабатывается. Таким образом, оператор создает «черную дыру» для рассматриваемого пункта назначения или пунктов назначения. Этот метод фильтрации обычно называют выражением «черная дыра». Следует отметить, что «черная дыра» трафика на основе пункта назначения вызывает отказ в обслуживании. Однако этот тип фильтрации может оказаться полезным, в частности, когда трафик, предназначенный для цели атаки, влияет на другие службы, которыми последний управляет или от которых он может получить выгоду. Некоторые операторы могут также предлагать аналогичную фильтрацию на основе IP-адресов источника атаки.

Использование сети доставки контента (CDN). Сеть доставки контента (CDN) – это серверная инфраструктура, распределенная в несколько дата-центров, и чья цель состоит в том, чтобы заменить услуги объекта, чтобы обслуживать его контент как можно ближе к пользователям. Таким образом, сети CDN имеют функцию кэширования и, в частности, позволяют повысить доступность ресурсов или даже увеличить скорость, с которой становятся доступными данные, как правило, веб-страницы или мультимедийные потоки. Для этого CDN в основном используют два метода:

– Метод геолокации исходного IP-адреса DNS-запросов, отправленных от клиента. Таким образом, можно направить последний к серверам, наиболее близким к его географическому положению;

– Метод адресации, известный как Anycast, который состоит в том, чтобы делиться одним и тем же IP-адрес между несколькими серверами, также называемыми узлами в контексте любой трансляции. IP-маршрутизация позволяет пользователю быть направленным на «ближайший» сервер или узел.

Распределение вычислительной нагрузки на большое количество серверов может помочь повысить устойчивость к некоторым DDoS-атакам. Например, атака, проводимая из источников, сосредоточенных в одном географическом регионе, затронет только узлы, обслуживающие этот регион. Кроме того, атака, исходящая из источников, распределенных по всему миру, может иметь меньшее воздействие, поскольку атака будет поглощена всеми серверами CDN. [2]

Перенаправление по протоколу DNS. Некоторые службы защиты полагаются на пересылку DNS. Цель – направить трафик в домен, например, example.com, на IP-адрес сервера провайдера защиты. Последний затем занимается фильтрацией трафика, а затем перенаправляет его в исходный пункт назначения. Эта операционная модель часто предлагается сетями CDN для защиты веб-серверов своих клиентов. Когда клиент желает получить доступ к веб-сайту www.example.com,

сначала он запрашивает DNS-сервер, чтобы узнать IP-адрес веб-сервера. Сервер отвечает IP-адресом одного из облачных узлов. Таким образом, трафик между клиентом и веб-сервером будет проходить через CDN, который, таким образом, может фильтровать трафик перед его возможной передачей на защищенный веб-сервер.

Некоторые сети CDN концентрируют трафик, покидающий их сеть и предназначенный для защищенного объекта, на ограниченном количестве четко идентифицированных узлов. Это позволяет защищенному объекту создавать и поддерживать белый список IP-адресов, которые могут связываться с его серверами [1].

Другие технические и организационные меры. Помимо конкретных защитных решений, существуют передовые методы, которые могут помочь повысить устойчивость к атакам типа «отказ в обслуживании». Среди них, в частности, можно отметить:

– сегментация сети объекта для облегчения фильтрации в случае атаки и возможная изоляция определенных подсетей или определенных серверов;

– реализация фильтрации на границе сети объекта для авторизации только тех потоков, которые необходимы последнему для работы.

Эти методы также помогают ограничить риск непреднамеренного участия в атаке отказа в обслуживании. Кроме того, необходимо создание специальной административной сети. Действительно, атака может значительно повлиять на сетевую инфраструктуру объекта и, таким образом, привести к трудностям доступа к оборудованию. Как минимум, административный трафик должен быть отмечен как приоритетный посредством реализации маркировки QoS (Качество обслуживания) [3].

Чтобы справиться с атакой типа «отказ в обслуживании», необходимо определить системы, которые могут стать целью, и знать группы, ответственные за администрирование этих

систем. Кроме того, крайне важно иметь соответствующие контакты внутри компании, с операторами транзита, а также с поставщиками услуг защиты от DDoS-атак.

Список использованных источников:

1. DoS-атака [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0
2. Что такое DDoS-атака [Электронный ресурс]. – URL: https://aws.amazon.com/ru/shield/ddos-attack-protection/
3. Защита от DDoS [Электронный ресурс]. – URL: https://www.xelent.ru/services-additional/zashchita-ddos/
4. DDoS-атака – что это такое? [Электронный ресурс]. – URL: https://ddos-guard.net/ru/terminology/attacks/ddos-ataka
5. Способы защиты от DDoS-атак [Электронный ресурс]. – URL: https://timeweb.com/ru/community/articles/sposoby-zashchity-ot-ddos-ataki-1

Ключові слова: DDoS, DDoS-атака, захист від DDoS-атак.
Ключевые слова: DDoS, DDoS-атака, защита от DDoS-атак.
Keywords: DDoS, DDoS attack, DDoS attack protection.

Научный руководитель: *к.т.н., доцент Соколов А. В.*

Саніцька Інна Валеріївна
Національний університет «Одеська юридична академія»,
студентка 4 курсу факультету кібербезпеки
та інформаційних технологій

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Інформаційна безпека – це такий стан захищеності інформаційної інфраструктури, включаючи також комп'ютери та інформаційно-телекомунікаційну інфраструктуру і інформацію, що в них знаходиться, який також забезпечує сталий розвиток особистості, суспільства і держави.