МАТЕМАТИЧЕСКИЕ МОДЕЛИ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СИСТЕМ ОТ DDOS-АТАК

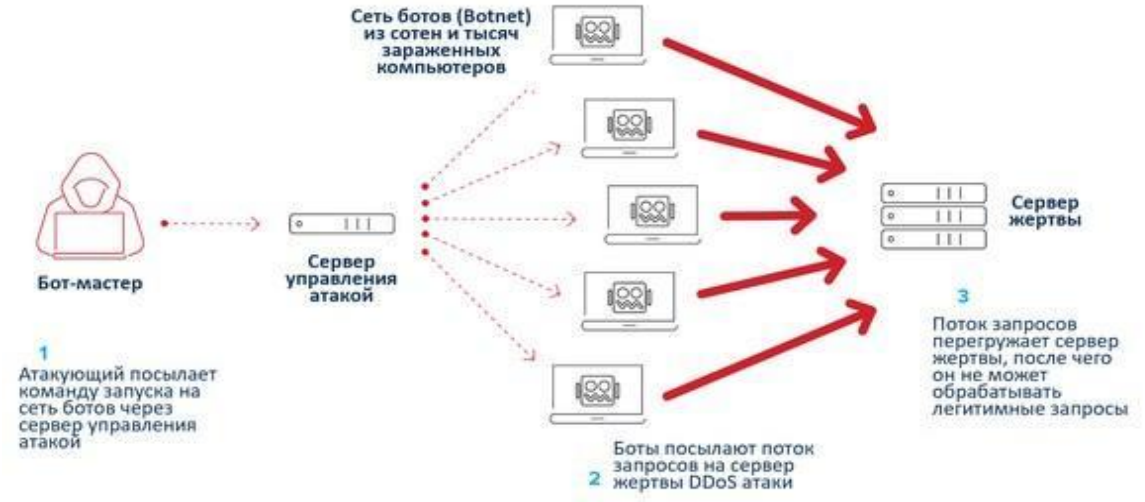
Насруллаев Нурбек Бахтийорович
PhD. Дотцент кафедри информационный безапосност, Нурафшонский филиал ТАТУ имени Мухаммада ал-Хоразми исполняющий обязанности директора
E-mail@: n.nasrullayev@tuit.uz
тел +998712386566
Артиков Нодирбек Ахмеджан угли
Ургенчский филиал ТАТУ имени Мухаммада ал-Хоразми 2-курс магистрант
E-mail@: artikovnodir18@gmail.com
тел +998999425033
https://doi.org/10.5281/zenodo.7970897

Аннотация: В данной статье представлена информация о видах киберугроз DDos компьютерным системам в сфере информационных технологий на сегодняшний день, их вреде и способах защиты.

Ключевые слова: Классификация DDoS-атак, Атаки уровня инфраструктуры, Атаки уровня приложения, Типы DDoS-атак, Методы защиты от DDoS-атак, Защита периметра сети.

Атаки типа «отказ в обслуживании» DoS (Denial of Service) – это перегрузка сети паразитным трафиком (т.н. флуд), когда на атакуемый ресурс отправляется большое количество злонамеренных запросов, из-за чего полностью «забиваются» все каналы сервера или вся полоса пропускания входного маршрутизатора. При этом передать легитимный трафик на сервер становится невозможно. Запросов может быть так много, что сервер не успевает их обрабатывать и переходит в режим «отказа в обслуживании». На жаргоне специалистов это называется «положить сервер».

Если такая атака ведется не от одного компьютера, а от многих, то такая атака называется распределенной атакой DDoS (Distributed DoS).



В общем случае DDoS-атаки можно разделить на типы в зависимости от того, на каком уровне модели взаимодействия открытых систем (OSI) происходит атака. Атаки на сетевом уровне (уровень 3), транспортном уровне (уровень 4), уровне представления (уровень 6) и уровне приложений (уровень 7) наиболее распространены.

Модель взаимодействия открытых систем (OSI)

#	Уровень 7	Приложение	Описание	Пример вектора
7	Приложение	Данные	Сетевой процесс в адрес приложения	флуд DNS-запросов, HTTP-флуд
6	Представление	Данные	Представление и шифрование данных	SSL-нарушение
5	*Сеанс*	*Данные*	*Сеанс связи между хостами*	*Н/Д*
4	Транспортный	Сегменты	Связь между конечными пунктами и надежность	SYN-флуд
3	Сетевой	Пакеты	Определение маршрута и логическая адресация	Атаки с отражением UDP-пакетов
2	*Канальный*	*Кадры*	*Физическая адресация*	*Н/Д*

1	*Физический*	*Биты*	*Среда передачи, сигнал и двоичные данные*	*Н/Д*

Классификация DDoS-атак

Рассматривая методы предотвращения таких атак, полезно разделить их на две группы: атаки уровня инфраструктуры (уровни 3 и 4) и атаки уровня приложения (уровни 6 и 7).

Атаки уровня инфраструктуры

К атакам уровня инфраструктуры обычно относят атаки на уровнях 3 и 4. Это наиболее распространенный тип DDoS-атак, который включает в себя такие векторы, как SYN-флуд, и другие атаки отражения, такие как UDP-флуд. Подобные атаки обычно массовые и направлены на то, чтобы перегрузить пропускную способность сети либо серверы приложений. Тем не менее, такой тип атак имеет определенные признаки, поэтому их легче обнаружить.

Атаки уровня приложения

К атакам уровня приложений обычно относят атаки на уровнях 6 и 7. Эти атаки менее распространены, но в то же время являются более сложными. Как правило, они не столь массовые, как атаки уровня инфраструктуры, но нацелены на определенные дорогостоящие части приложения и приводят к тому, что оно становится недоступным для реальных пользователей. В качестве примера можно привести поток HTTP-запросов на страницу входа в систему, дорогой API поиска или даже потоки XML-RPC Wordpress (также известные как атаки Wordpress Pingback).

Атаки 3-4 уровня OSI

Это атаки на сетевом и транспортном уровнях. Злоумышленники «забивают» каналы передачи большим количеством передаваемых пакетов. Канал не может справиться с нагрузкой и выдает ошибку «отказ в доступе». DDoS-атаки могут использовать недостатки сетевых протоколов, перегружая сервер, в результате чего сервер перестает отвечать на запросы.

Атаки 7 уровня OSI

Атаки на уровне приложений потребляют не только сетевые ресурсы, но и ресурсы сервера. Сервер не выдерживает нагрузку, что приводит к его недоступности. Атака при этом направлена непосредственно на операционную систему или приложение с целью вынудить их превысить лимит вычислительной мощности сервера. При этом атакам подвергаются

конкретные приложения, сервисы и службы. Атаки могут продолжаться длительное время (несколько часов или дней).

Типы DDoS-атак

HTTP-флуд: самый простой вид запросов, например, при помощи HTTP-заголовка пакета, который указывает запрашиваемый ресурс сервера. Злоумышленник может использовать сколько угодно заголовков, придавая им нужные свойства. При DDoS-атаке HTTP-заголовки могут изменяться, делая их труднораспознаваемыми для выявления атаки. Кроме того, HTTP-запросы атаки могут передаваться по защищенному протоколу HTTPS. В этом случае все пересылаемые между клиентом (злоумышленником) и сервером данные шифруются. При этом «защищенность» идет атакующему только на пользу: чтобы выявить злонамеренный запрос, сервер должен сначала расшифровать его. То есть расшифровывать приходится весь поток запросов, которых во время DDoS-атаки поступает очень много. Это создает дополнительную нагрузку на сервер-жертву, что приводит к исчерпанию его вычислительной мощности.

SYN-флуд (TCP/SYN): устанавливает полуоткрытые соединения с узлом. Когда сервер-жертва принимает SYN-пакет синхронизации через открытый порт, он должен послать в ответ на сервер-источник запроса пакет подтверждения SYN-ACK и открыть соединение. После этого запроса сервер-источник должен послать на сервер пакет подтверждения ACK, однако злоумышленник не посылает это подтверждение. Соединения остаются полуоткрытыми до истечения тайм-аута. Очередь на подключение на атакуемом сервере переполняется и новые клиенты не могут установить соединение с сервером.

MAC-флуд: злоумышленник посылает поток пустых фреймов Ethernet с разными MAC-адресами в каждом. Коммутаторы сети рассматривают каждый MAC-адрес в отдельности и резервируют ресурсы под каждый из них. Когда вся память коммутатора использована, он либо перестает отвечать, либо останавливает работу. Иногда атака MAC-флудом может удалять таблицы маршрутизации на узлах сети, таким образом нарушая работу всей сети, а не только одного сервера.

Ping of Death: мастер-бот Ping of Death посылает злонамеренные пинг-запросы через различные IP-протоколы на атакуемый сервер, что приводит к его перегрузке. В настоящее время такие атаки редки. Пропускная способность сетей значительно повысилась, а для таких атак нужно много ресурсов – зараженных ботов.

Smurf Attack: разновидность Ping of Death. Этот вид атаки использует протокол Интернет (IP) и протокол управляющих сообщений ICMP (Internet Control Message Protocol), на которых работает зловредная программа Smurf. Она подменяет IP-адрес атакующего и пингует IP-адреса в корпоративной сети, оставляя на них полуоткрытые соединения.

Fraggle Attack: использует большие объемы трафика UDP на вещательной сети маршрутизатора. Эта атака работает аналогично Smurf-атаке, но вместо протокола ICMP использует вещательный протокол UDP.
Slowloris. Атака Slowloris направлена на веб-сервер. Атакующий сервер подключается к целевому серверу и оставляет это подключение полуоткрытым настолько долго, насколько это возможно, а затем размножает эти полуоткрытые соединения. Закрытие таких соединений атакуемым сервером по таймауту происходит медленнее, чем установка новых соединений. Противодействовать этой атаке довольно сложно, поскольку сложно отследить источник атаки.

NTP-усиление. Атака использует серверы протокола сетевого времени NTP (Network Time Protocol), который используется для синхронизации компьютерных часов в сети. Цель атаки – перегрузка трафиком UDP. При этой атаке атакуемый сервер отвечает, посылая UDP-трафик на подмененный злоумышленником IP-адрес. «Усиление» означает, что объем ответного UDP-трафика много больше запроса. Поэтому сеть быстро перегружается бесполезным трафиком, а ее узлы останавливают работу.

Pulse Wave. Главная опасность пульсирующих атак Pulse wave заключается в методике периодических всплесков трафика. Обычная DDoS-атака выглядит как постепенно нарастающий поток вредоносного трафика. Pulse wave представляет собой серию коротких, но мощных импульсов, происходящих с определенной периодичностью.

APDoS. Усовершенствованная повторяющаяся DoS-атака APDoS (Advanced Persistent DoS) нацелена на нанесение максимального вреда атакуемому серверу. Он использует механизмы HTTP-флуда, SYN-флуда и других видов атак. При этом посылаются миллионы запросов в секунду. Такая атака может длиться неделями, поскольку злоумышленник все время меняет тактику атаки, типы атаки, чтобы обмануть средства противодействия атакуемой стороны.

Методы защиты от DDoS-атак

Уменьшение зон, доступных для атаки

Одним из первых методов нейтрализации DDoS-атак является сведение к минимуму размера зоны, которую можно атаковать. Подобный прием ограничивает возможности злоумышленников для атаки и обеспечивает возможность создания централизованной защиты. Необходимо убедиться, что доступ к приложению или ресурсам не был открыт для портов, протоколов или приложений, взаимодействие с которыми не предусмотрено. Таким образом, сведение к минимуму количества возможных точек для атаки позволяет сосредоточить усилия на их нейтрализации. В некоторых случаях этого можно добиться, разместив свои вычислительные ресурсы за сетями распространения контента (CDN) или балансировщиками нагрузки и ограничив прямой интернет-трафик к определенным частям своей инфраструктуры, таким как серверы баз данных. Также можно использовать брандмауэры или списки контроля доступа (ACL), чтобы контролировать, какой трафик поступает в приложения.

План масштабирования

Двумя основными элементами нейтрализации крупномасштабных DDoS-атак являются пропускная способность (или транзитный потенциал) и производительность сервера, достаточная для поглощения и нейтрализации атак.

Транзитный потенциал. При проектировании приложений необходимо убедиться, что поставщик услуг хостинга предоставляет избыточную пропускную способность подключения к Интернету, которая позволяет обрабатывать большие объемы трафика. Поскольку конечная цель DDoS-атак – повлиять на доступность ресурсов или приложений, необходимо

размещать их рядом не только с конечными пользователями, но и с крупными узлами межсетевого обмена трафиком, которые легко обеспечат вашим пользователям доступ к приложению даже при большом объеме трафика. Работа с интернет-приложениями обеспечивает еще более широкие возможности. В этом случае можно воспользоваться сетями распространения контента (CDN) и сервисами интеллектуального преобразования адресов DNS, которые создают дополнительный уровень сетевой инфраструктуры для обслуживания контента и разрешения DNS-запросов из мест, которые зачастую расположены ближе к конечным пользователям.

Производительность сервера. Большинство DDoS-атак являются объемными и потребляют много ресурсов, поэтому важно иметь возможность быстро увеличивать или уменьшать объем своих вычислительных ресурсов. Это можно обеспечить, используя избыточный объем вычислительных ресурсов или ресурсы со специальными возможностями, такими как более производительные сетевые интерфейсы или улучшенная сетевая конфигурация, что позволяет поддерживать обработку больших объемов трафика. Кроме того, для постоянного контроля и распределения нагрузок между ресурсами и предотвращения перегрузки какого-либо одного ресурса часто используются соответствующие балансировщики.

Сведения о типичном и нетипичном трафике

Каждый раз, когда обнаруживается повышение объема трафика, попадающего на хост, в качестве ориентира можно брать максимально возможный объем трафика, который хост может обработать без ухудшения его доступности. Такая концепция называется ограничением скорости. Более продвинутые методы защиты соответственно обладают дополнительными возможностями и могут интеллектуально принимать только трафик, который разрешен, анализируя отдельные пакеты. Для использования подобных средств необходимо определить характеристики хорошего трафика, который обычно получает целевой объект, и иметь возможность сравнивать каждый пакет с этим эталоном.

Развертывание брандмауэров для отражения сложных атак уровня приложений

Против атак, которые пытаются использовать уязвимость в приложении, например против попыток внедрения SQL-кода или подделки межсайтовых запросов, рекомендуется использовать Web Application

Firewall (WAF). Кроме того, из-за уникальности этих атак вы должны быть способны самостоятельно нейтрализовать запрещенные запросы, которые могут иметь определенные характеристики, например могут определяться как отличные от хорошего трафика или исходить из подозрительных IP-адресов, из неожиданных географических регионов и т. д. Чтобы нейтрализовать происходящие атаки, иногда может быть полезно получить поддержку специалистов для изучения характеристик трафика и создания индивидуальной защиты.

Однократное выделение серверу полосы пропускания «с запасом». Чем шире полоса у веб-сервера, тем обычно лучше. Таким образом сервер может выдерживать резкие и неожиданные всплески трафика, которые могут быть, например, результатом рекламной кампании. Но даже если заложить запас в 100 %, или 500 %, это вряд ли спасет от DDoS-атаки. Однако это может дать некоторое время на распознавание источника и типа атаки и принятие мер до того, как сервер «ляжет» полностью.

Защита периметра сети. Есть несколько технических мер, которые можно предпринять для частичного ограничения эффекта атаки. Многие из них довольно просты и требуют лишь регулировки сетевых настроек. Например:

Ограничить скорости маршрутизатора, чтобы предотвратить остановку сервера.

Установить фильтры на маршрутизаторе для сброса пакетов от распознанного источника атаки.

Установить таймаут на полуоткрытые соединения (от которых в течение времени таймаута не получен подтверждающий ответ источника запроса).

Сбрасывать пакеты с подмененными IP-адресами и вообще пакеты необычной структуры.

Установить более низкие пороги сброса для SYN-, ICMP-, и UDP-флуда.

Однако все эти меры хорошо известны и хакерам, и они изобретают все новые способы атак и увеличивают их интенсивность. Но все же эти меры помогут выиграть время на распознавание атаки и принятие мер до наступления фатальной ситуации.

Шансы на предотвращение DDoS-атаки значительно увеличиваются, если веб-сервер расположен в дата-центре, а не в корпоративной сети предприятия. В дата-центрах обычно и входная полоса шире, и имеются мощные маршрутизаторы, которые не всякая организация может себе позволить, а также и персонал имеет больше опыта в предотвращении

атак. По крайней мере, другие серверы организации (email, VoIP и пр.) не подвергнутся воздействию атаки.

Заключение

С развитием ИТ-технологий в киберпространстве появились новые угрозы. Злоумышленники совершенствуют свои инструменты и находят все более изощренные способы достижения своих целей. Для обнаружения атак на ранней стадии необходимо определить различные технологии анализа и обнаружения вредоносной активности, а также различные технологии прогнозирования потенциальных несанкционированных воздействий. Но при успешной атаке внедряются технологии для определения последствий взлома информационных систем. Необходимо учитывать технологии, актуальные угрозы и риски, киберугрозы и риски на законодательном уровне, а также область соблюдения требований безопасности. Использование серьезного подхода к выбору средств обнаружения позволяет построить более эффективную систему защиты информации и предотвратить большой ущерб при компьютерной атаке.

Использованные источники:

1.https://aws.amazon.com/ru/shield/ddos-attack-protection/08.05.2022 21:04
2.https://itelon.ru/blog/zashchita-servera-ot-ddos-atak/
https://itelon.ru/upload/img/20-01-2021/1.jpg 08.12.2022 00:23