Ростелеком
Солар

Отчет о DDoS-атаках на российские компании

за 1–3 квартал 2021 года

rt-solar.ru

ОГЛАВЛЕНИЕ

Введение

Минувший 2020 год принес нам пандемию, самоизоляцию, удаленку и, как следствие, увеличение спроса на различные онлайн-услуги. В 2021 году, несмотря на постепенное возвращение к офлайн-жизни, востребованность интернет-сервисов остается высокой, а кибепреступники продолжают активно атаковать различные ресурсы. Один из самых популярных инструментов хакеров – DDoS (атаки типа «отказ в обслуживании»). С одной стороны, несложную и маломощную атаку могут организовать даже хакеры-любители, так как для этого им не нужно специальное оборудование или финансовые вложения.

С другой, в руках профессиональных злоумышленников, которые могут собрать масштабный ботнет из десятков тысяч устройств, DDoS становится мощным оружием, которое может вывести из строя даже ресурсы крупной компании.

Эксперты «Ростелекома» подготовили отчет о том, как поменялся ландшафт DDoS-атак на российские компании на фоне постепенного выхода с удаленки и возвращения к привычной жизни. Аналитика составлена на основе данных об атаках, наблюдаемых специалистами Центра кибербезопасности и защиты «Ростелекома» с января по сентябрь 2021 года.

ДЛЯ ОТЧЕТА БЫЛА ПРОАНАЛИЗИРОВАНА ИНФОРМАЦИЯ ПОЧТИ О 300 КОМПАНИЯХ ИЗ РАЗЛИЧНЫХ ОТРАСЛЕЙ, ВКЛЮЧАЯ ТЕЛЕКОМ, РИТЕЙЛ, ФИНАНСОВЫЙ И ГОСУДАРСТВЕННЫЙ СЕКТОРА. ВСЕ ВЫЯВЛЕННЫЕ АТАКИ БЫЛИ ОТРАЖЕНЫ ЭКСПЕРТАМИ КОМПАНИИ.

Количество атак и отрасли

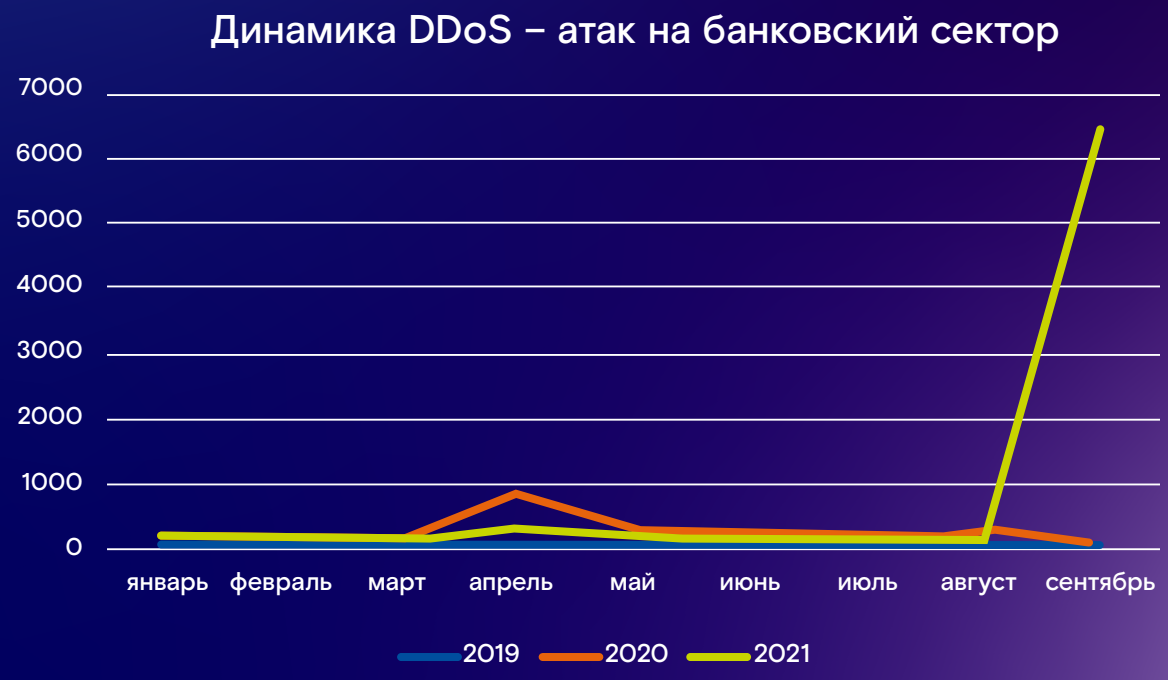
За первые три квартала 2021 года количество DDoS-атак на российские организации **выросло почти в 2,5 раза.** Этот тренд наметился еще в 2020 году, когда большинство компаний перешло на удаленный режим работы, а люди боялись выходить из дома из-за пандемии и предпочитали получать многие услуги, включая покупку товаров, обучение и развлечения, через интернет.

DDoS-атака в случае успеха хакеров, может нанести серьезный удар по организации.
Например:

- Клиенты, не получив доступ к сайту, могут перейти к конкурентам, а сам сайт может пропасть на время из поисковой выдачи;
- Могут быть атакованы не только публичные ресурсы, но и непубличные, которые используют сотрудники для работы (парализована почта или удаленный доступ к рабочему месту), что приведет к нарушению бизнес-процессов;
- Также хакеры часто атакуют ресурсы, являющиеся основным инструментом бизнеса, что может привести к серьезным последствиям (например, внутренние банковские ресурсы, которые отвечают за транзакции и т.п.);
- Хакеры могут потребовать крупный выкуп, чтобы прекратить DDoS-атаку на сайт жертвы;
- Простая DDoS-атака может стать дымовой завесой для более серьезного инцидента, и пока ИБ-специалисты пытаются восстановить работу сервера, хакеры могут похитить конфиденциальные данные клиентов или корпоративную информацию;

Банки

За три квартала 2021 года **в 3,5 раза** выросло количество DDoS-атак на банки и финансовые организации, при этом пик активности хакеров пришёлся на сентябрь, когда было совершено почти **90% всех атак**. Всплеск DDoS-атак на банковский сектор в этот период фиксировали и другие провайдеры сервисов кибербезопасности, в то же время публичные источники отмечали, что ряд финансовых структур столкнулся с простоями своих онлайн-ресурсов. В том числе, DDoS-атаки были направлены на крупнейшие банки из ТОП-20. На бизнес-процессы заказчиков «Ростелекома» данная серия атак не повлияла, так как была своевременно отражена.



Онлайн-торговля

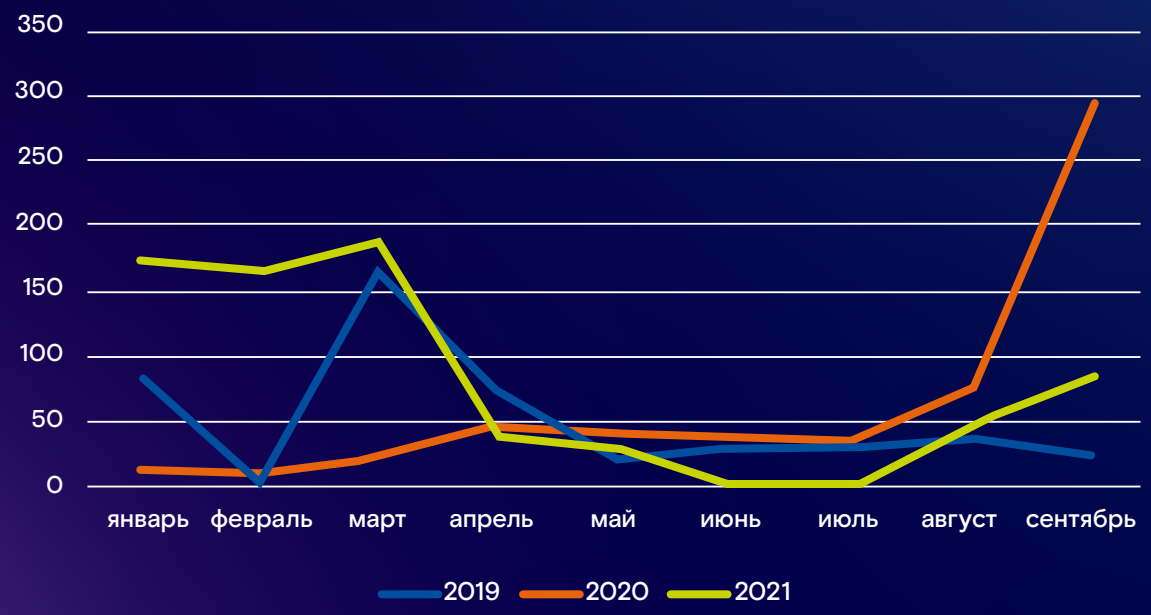
Ритейл остается привлекательной целью киберпреступников. За первые три квартала 2021 года количество DDoS-атак на этот сегмент выросло на 20% в сравнении с аналогичным периодом прошлого года. При этом в 2020 году эксперты «Ростелеком-Солар» уже фиксировали 2-кратный рост DDoS-инцидентов в отношении онлайн-магазинов. Тогда интерес хакеров к этой сфере был связан с резким увеличением спроса на услуги онлайн-магазинов в период самоизоляции и пика пандемии. Как следствие, увеличилось количество пользователей онлайн-магазинов и объем их персональных данных, хранящихся в сети.
В то же время недобросовестные конкуренты стали активнее использовать DDoS, чтобы испортить репутацию своим конкурентам и сделать их сайты недоступными для покупателей.

При этом конкуренция на рынке остается высокой, а онлайн-шопинг востребован, поэтому можно прогнозировать дальнейший рост DDoS-атак на отрасль.

Пик активности хакеров в 2021 году пришелся на начало года, а наибольшее количество DDoS-атак было зафиксировано в марте. После определенного затишья, с августа уровень атак начал расти, что может быть связано с подготовкой к началу учебного года и нового бизнес-сезона, а значит, с необходимостью обновить гардероб, технику и т.п.

Можно предположить, что до нового года мы увидим возрастающий тренд по количеству DDoS-атак, связанный с акцией «Черная пятница» и предновогодними распродажами, которые начинаются в ноябре и продолжаются до февраля следующего года.

Динамика DDoS – атак на онлайн – торговлю



Госсектор

Также сохраняется рост числа атак на госсектор – на 17% за три квартала 2021 года в сравнении с аналогичным периодом 2020 года. Этот тренд также берет начало в 2020 году, когда число DDoS-атак на государственные ресурсы выросло в три раза.
Тогда резкая активность хакеров в отношении госсектора совпала с введением платформ для мониторинга передвижения граждан на фоне панде-мии, объявлением о дополнительных мерах финансовой поддержки, которые можно было оформить онлайн и т.п.

В 2021 году наибольшая активность злоумышленников пришлась на март, когда произошло в 2,5 раза больше атак, чем годом ранее. Также в 2 раза выросло число DDoS-атак в августе и сентябре в сравнении с аналогичным периодом предыдущего года. Не исключено, что атаки на государственные ресурсы могли быть связаны с подготовкой к выборам в Государственную думу, так как именно на август - начало сентября пришлась наиболее активная агитация за кандидатов. Таким образом DDoS мог использоваться злоумышленниками для дискредитации кандидатов или из хулиганских побуждений.

Динамика DDoS – атак на госсектор

Другие отрасли

В то же время есть сферы, в которых в отчетный период количество DDoS-атак сократилось. Например, в игровом сегменте падение составило 35%. Но это говорит не столько об отсутствии интереса хакеров к данной отрасли, сколько о корректировке тренда после резкого всплеска (в три раза) в период пандемии. Тогда режим самоизоляции по всему миру значительно нарастил аудиторию онлайн-игр и киберспорта, который на время заменил зрителям реальные соревнования и чемпионаты. Это обострило конкуренцию между площадками, и DDoS, позволяющий вывести из строя сайт конкурента, оказался очень востребован. Однако если сравнить показатели 2019 года, то виден двукратный рост DDoS-атак за последние два года.

Также за отчетный период на четверть упало количество атак на дата-центры, что компенсирует аномальный всплеск предыдущего года. В 2020 году рост DDoS-атак на этот сегмент был, скорее всего, связан с пандемией и переходом на удаленную работу.

Тогда многие компании запускали собственные онлайн-ресурсы, так как предоставлять услуги офлайн стало невозможно, и самый быстрый и доступный вариант организовать онлайн-канал коммуникации с клиентом заключался в аренде физического или виртуального сервера в дата-центре. Некоторые компании, у которых были собственные серверы, могли также переместить ресурсы в ЦОД, чтобы отправить администраторов на «удаленку» и предоставить им возможность дистанционного управления этими серверами. Кроме того, эта перестройка происходила быстро – дата-центрам было сложно обеспечить эффективную защиту на фоне резкого скачка числа клиентов, что делало их привлекательной целью для хакеров. Однако дата-центры, очевидно, оперативно подняли уровень ИБ, а потому и DDoS в этой сфере стал не таким эффективным хакерским инструментом.

Типы атак и мощность

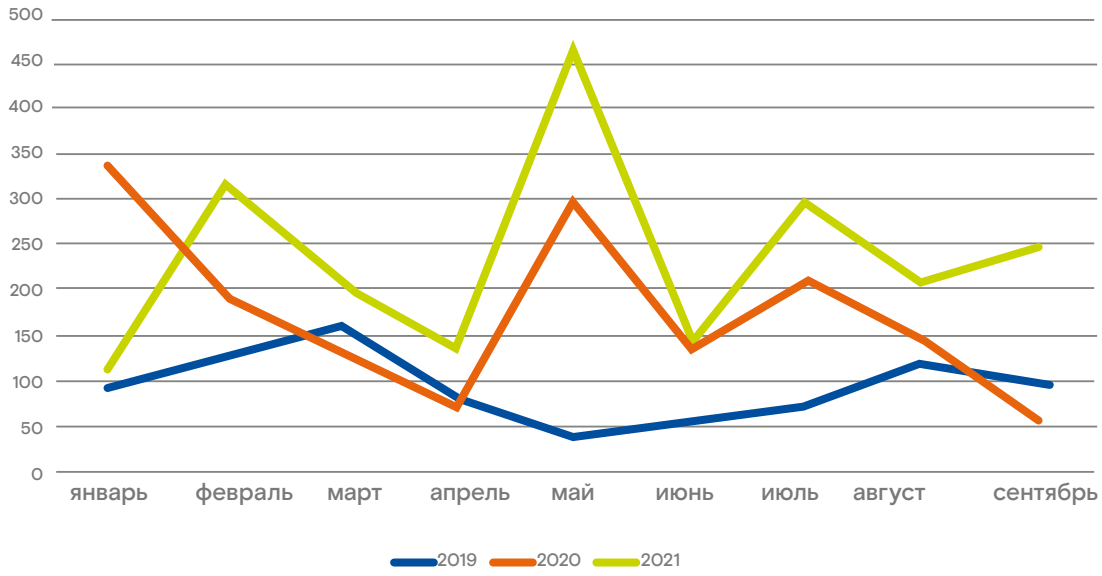
Вместе с количеством атак выросла и их средняя мощность – на 26%. Самая мощная атака была зафиксирована в мае и ее мощность составила **462 Гбит/с**, что на треть превышает пиковое значение первых трех кварталов 2020 года.

В результате специалисты компании совместно с экспертами Национального координационного центра по компьютерным инцидентам (НКЦКИ) обнаружили 45 тыс. сетевых устройств, идентифицировали их географическое местоположение и изолировали от ботнета, не допустив таким образом расширения сети. Также удалось выяснить, что для взлома устройств хакеры использовали вредоносное ПО Glupteba, которое обычно находится в арсенале профессиональных злоумышленников.

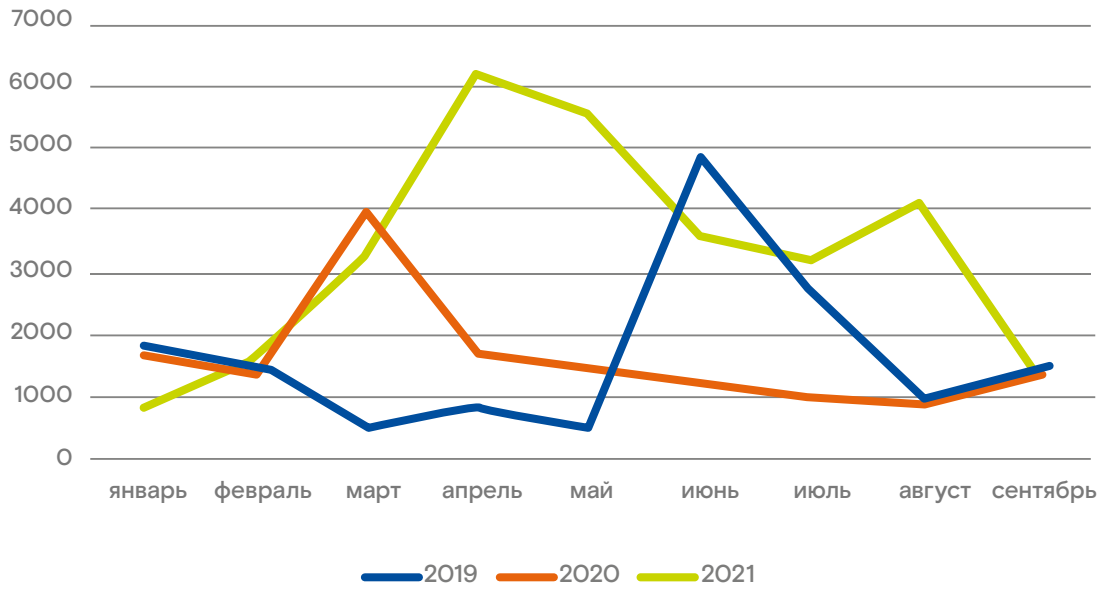
Для увеличения мощности атак злоумышленники продолжают активно использовать ботнеты для организации DDoS, при этом количество используемых устройств постоянно растет. В частности, в сентябре хакеры организовали крупнейшую DDoS-атаку с помощью ботнета Meris, предположительный масштаб которого составляет 200 тыс. устройств. Большая часть сети состоит преимущественно из оборудования MikroTik, которое широко применяется домашними пользователями для подключения к интернету. Экспертам центра раннего выявления киберугроз Solar JSOC CERT компании «Ростелеком-Солар» удалось получить и проанализировать команды, которые используются для управления зараженными устройствами.

Продолжительность DDoS также увеличивается. Самая долгая атака в отчетный период длилась почти 4,5 дня. Годом ранее этот показатель за первые три квартала составил почти 3 дня.

Мощность атак в 1-3 квартале 2019-2021 гг



Самые долгие атаки 1-3 квартале 2019-2021 гг



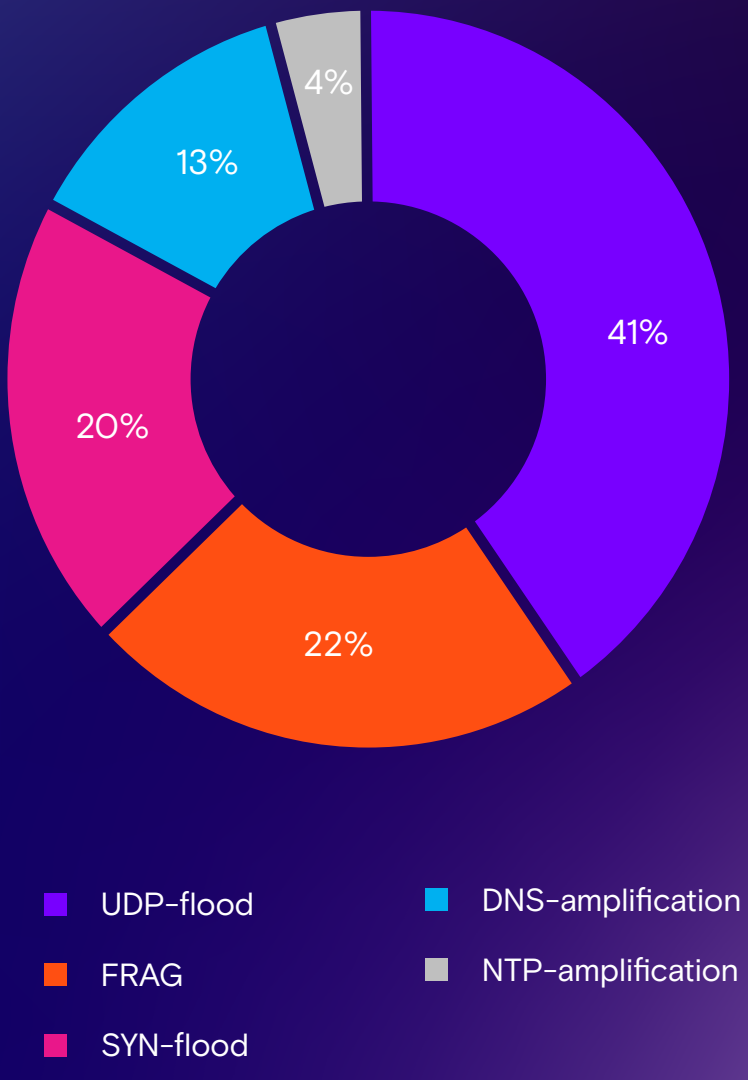
Техники, которые используют хакеры для реализации DDoS, остаются неизменными уже не первый год. В половине случаев злоумышленники использовали **UDP flood**. Его суть заключается в том, что сервер-жертва получает огромное количество UDP-пакетов в единицу времени от широкого диапазона IP-адресов, которые занимают всю полосу пропускания. В итоге канал сервера оказывается перегружен и не может обрабатывать другие запросы.

Также популярным остается **SYN flood**, который использовался почти в трети атак. В этом случае злоумышленник отправляет на целевой сервер массу SYN-пакетов (то есть запросов на подключение). Сервер жертвы резервирует ресурсы на ответ, открывая соединение на своей стороне, и ожидает завершения установки соединения, которого так и не происходит. В это время злоумышленник продолжает отправлять запросы, создавая полуоткрытые соединения, которые переполняют очередь подключений, вынуждая сервер отказывать в обслуживании реальным клиентам.

В топ-3 техник также входят **DDoS-атака фрагментированными пакетами (FRAG)**. Такая атака предполагает передачу в адрес жертвы множества фрагментированных пакетов данных. Сервер безуспешно пытается их обработать, так как не может собрать фрагменты. Жертва тратит чрезмерное количество ресурсов, что вызывает сбой. Это более сложная техника, чем усиление атаки через амплификацию, но организовать эффективный FRAG можно в том числе с помощью масштабного ботнета. Это еще раз указывает на то, что DDoS-атаки активно использовали уже не хакеры-любители, как это было в период пандемии, а более профессиональные злоумышленники. Примечательно, что годом ранее этот тип атак применялся в два раза реже.

Также злоумышленники использовали обычную **DNS-амплификацию или NTP-амплификацию,** которые считаются достаточно простыми способами организации DDoS-атак. Их простота заключается в том, что хакеры задействуют серверы, находящиеся в открытом доступе. При DNS-амплификации злоумышленник посылает запрос (обычно короткий) уязвимому DNS-серверу, который отвечает уже значительно большим по размеру пакетом. В качестве исходного IP хакеры ставят адрес компьютера жертвы (IP spoofing), куда уязвимый DNS-сервер и посылает ответы, пока полностью не парализует его ресурсы. А при NTP-амплификации злоумышленник неоднократно отправляет запрос «предоставить контрольный список» на NTP-сервер, одновременно подменяя свой IP-адрес на адрес сервера-жертвы. Отправляемый NTP-сервером ответ по объему значительно превосходит запросы, что приводит к загруженности канала связи.

Распределение атак по типам 1-3 квартале 2021 года



Выводы и советы

1 Количество DDoS-атак на российские компании продолжает расти: за первые три квартала 2021 года этот показатель увеличился в **2,5** раза.

2 Вместе с количеством растет мощность и продолжительность атак. Самая мощная была зафиксирована в мае и ее мощность составила 462 Гбит/с, что на треть превышает пиковое значение первых трех кварталов 2020 года. А самая долгая в отчетный период атака длилась почти 4,5 дня. Годом ранее этот показатель за первые три квартала составил почти 3 дня.

3 Хакеры продолжают использовать масштабные ботнеты для увеличения мощности атак. На отчетный период пришлась активность ботнета Meris, предположительный масштаб которого составляет 200 тыс. устройств.

4 В фокусе внимания злоумышленников: финансовая отрасль, госсектор, онлайн-торговля.

5 Наиболее распространенные типы атак: UDPflood, SYN flood и атаки фрагментированными пакетами (FRAG), которые обычно организуют с помощью ботнетов.

Чтобы инфраструктура выдержала

DDoS-атаку следует:

1 Отделить веб-приложения от остальных ресурсов организации, разместив их на разных площадках компании или в разных дата-центрах.

При этом подключение к ЦОДам должно осуществляться разными операторами связи. В случае DDoS-атаки это обеспечит отказоустойчивость инфраструктуры.

2 К решению по защите типа Anti-DDoS стоит добавить Web Application Firewall (WAF), то есть межсетевой экран уровня веб-приложений. Он защитит не только от DDoS-атак на приложение, но и от сложных угроз, например, попыток кражи и изменения данных приложений. Это особенно актуально для компаний, которые собирают много персональных данных клиентов, например, для ритейла или банков.

3 Выбирать для защиты от DDoS-атак надежного провайдера, который гарантирует, что его услугами пользуются только легальные сайты и который оперативно взаимодействует с регуляторами. Дело в том, что провайдеры раздают клиентам адреса в случайном порядке. Если на «соседнем» адресе расположен нелегальный сайт, нарушающий законодательство, то его блокировка может повлиять на доступность и ваших ресурсов.

4 Заказывать услуги по Anti-DDoS у провайдера, который уже имеет портфолио исполнителя, внимательно исследует защищаемую инфраструктуру, имеет опыт в определении корреляций между событиями ИБ разных сервисов.

Ростелеком
Солар

rt.ru
rt-solar.ru

info@rt-solar.ru
+7 (499) 755-07-70

Задать вопрос или
попробовать сервис

presale@rt-solar.ru