Ростелеком
Солар

DDoS-атаки на онлайн-ритейл

ОТЧЕТ ОБ ИЗМЕНЕНИИ ИБ-ЛАНДШАФТА ПОД ВЛИЯНИЕМ COVID-19 В 2020 ГОДУ

ОГЛАВЛЕНИЕ

1 **Введение** 3

2 **Основные цифры** 4

3 **Как хакеры атаковали онлайн-ритейл** 5

3.1 Количество атак 5

3.2 Основные инструменты злоумышленников 6

3.3 Цели и ущерб от DDoS-атак 8

4 **Выводы и прогнозы** 10

ВВЕДЕНИЕ

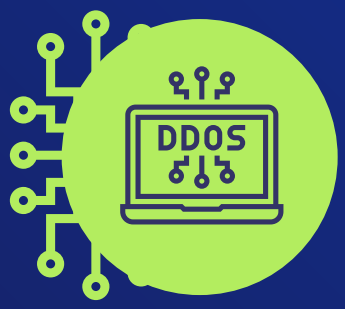
Распространение COVID-19 и введение различных карантинных мер повлияло на все сферы жизни, изменив наши потребительские привычки. За короткий период спрос на услуги интернет-магазинов увеличился в разы. Но резкий взлет популярности этого сегмента спровоцировал пропорциональный рост количества кибератак на него. Традиционно в качестве основного инструмента против онлайн-ритейла киберпреступники выбрали DDoS-атаки, которые способны сделать сайт магазина недоступным для покупателей.

Эксперты «Ростелекома» подготовили отчет о том, как изменился ландшафт DDoS-атак на сферу онлайн-торговли под влиянием COVID-19. Аналитика составлена на основе данных об атаках, наблюдаемых специалистами Центра кибербезопасности и защиты «Ростелекома» с января по декабрь 2020 года. В выборку включены как ритейлеры, которые ведут свой бизнес исключительно онлайн, так и офлайн-магазины, которые предоставляют услуги дистанционного заказа товаров через веб-приложения и сайты.

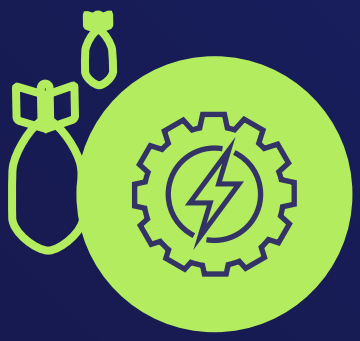
ОСНОВНЫЕ ЦИФРЫ

В январе-декабре 2020 года:

в 2 раза выросло количество DDoS-атак на сегмент онлайн-торговли в сравнении с аналогичным периодом прошлого года



пик активности хакеров пришелся на 4-й квартал, когда произошло почти 40% всех DDoS-атак



более 40 Гбит/с составила мощность самой сильной атаки

более 6 часов длилась самая продолжительная атака

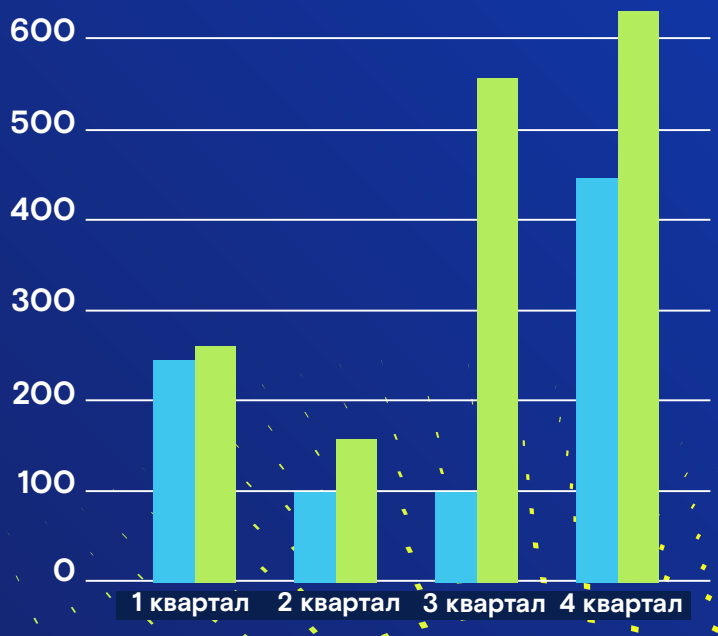
КАК ХАКЕРЫ АТАКОВАЛИ ОНЛАЙН-РИТЕЙЛ

КОЛИЧЕСТВО АТАК

Онлайн-торговля находится в фокусе внимания киберпреступников уже не первый год. Значение этой отрасли возросло на фоне распространения COVID-19 и введения различных карантинных мер. Люди стали чаще заказывать продукты и товары онлайн, опасаясь скопления покупателей в обычных магазинах, а сами ритейлеры начали активнее осваивать формат дистанционной торговли. На фоне роста популярности сегмента увеличилось и количество атак на него.
Так, за 2020 год количество DDoS-атак на онлайн-магазины возросло в 2 раза.

При этом резкий рост активности злоумышленников начинается во втором квартале 2020 года, что совпадает с введением первых карантинных мер в стране. Но даже после частичного снятия ограничений большинство граждан, очевидно, остались на «удаленке» и продолжили заказывать товары и еду через интернет.

Пик количества атак совпадает с периодом онлайн-распродаж, который приходится на 4-й квартал года. В это время онлайн-ритейлеры проводят акцию «Черная пятница», а также предлагают скидки на подарки в преддверии новогодних праздников. Всплеск DDoS-атак в конце года является традиционным явлением, но в 2020 году активность хакеров в этот период, как и в течение всего года, была выше показателей прошлых лет.



ОСНОВНЫЕ ИНСТРУМЕНТЫ ЗЛОУМЫШЛЕННИКОВ

В отчетный период при атаках на ритейл злоумышленники отдавали предпочтение простым и дешевым методам организации DDoS.

В частности, они взяли на вооружение атаки с амплификацией (то есть с усилением), которые годом ранее в этой отрасли применялись реже.

Если раньше более чем 80% атак на онлайн-ритейл приходилось на UDP flood, то в 2020 году его доля сократилась до четверти.

Суть UDP flood 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.

SYN flood, на который годом ранее приходилось менее 10% атак, в 2020-м сравнялся по количеству с UDP flood. Популярность SYN flood в принципе растет с каждым годом.

По оценке «Ростелекома», приведенной выше, в 2017 году такие атаки составляли только 10% от общего объема DDoS-атак по всем отраслям, а в 2019 году – уже 27%. Суть SYN flood заключается в том, что злоумышленник отправляет на целевой сервер массу SYN-пакетов (то есть запросов на подключение к серверу). 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.

Также в отчетный период злоумышленники часто применяли атаки типа TCP Reset flood, при которой нападающий разрывает соединение между сервером интернет-магазина и покупателем, направляя им фальшивые сообщения,

о том, что была обнаружена ошибка и требуется прекратить загрузку данных. Злоумышленник пересылает это сообщение много раз подряд, что делает невозможным установить соединение с сервером.

Таким образом, на фоне резкого увеличения спроса на онлайн-услуги, злоумышленники стали искать быстрые и дешевые методы организации DDoS-атак «здесь и сейчас». При этом киберпреступники делали ставку на их длительность, чтобы «измотать» жертву и наверняка вывести из строя ее ресурсы. По нашей оценке, самая продолжительная атака превышала 6 часов. Мощность DDoS-атак за год также увеличилась примерно в 10 раз.

Так, самая сильная атака на онлайн-торговлю в 2020 году превысила 40 Гбит/с. Однако на фоне общего ландшафта DDoS-атак такая мощность является относительно низкой. В 2019 году объемы самых мощных атак, которые эксперты «Ростелекома» наблюдали на своей сети, колебались в диапазоне от 60 до 400 Гбит/с.

ЦЕЛИ И УЩЕРБ ОТ DDOS-АТАК

Цели любой DDoS-атаки – с помощью огромного количества запросов нарушить работу сайта или другого интернет-ресурса, сделав его недоступным для обычных пользователей. В ритейле это приводит к тому, что покупатели не могут оформить и оплатить свой онлайн-заказ или даже зайти в каталог интернет-магазина.

Самая популярная причина для организации подобной атаки – это конкурентные войны. Нечистые на руку бизнесмены «заказывают» хакерам других игроков рынка.
В условиях жесткой конкуренции и неработающего сайта клиент с большой вероятностью воспользуется услугами другого интернет-магазина. Вдобавок к этому поисковые системы перестают ротировать недоступные сайты в своей выдаче. А значит, бюджет на рекламу и продвижение потрачен впустую, не говоря уже о драматичном снижении трафика.

DDoS-атака может нарушить не только работу пользовательского сайта, но и внутренних ресурсов компании, если те обрабатываются на атакованном сервере. Эта проблема особенно актуальна для онлайн-ритейла, в котором многие игроки рынка представляют СМБ-сегмент. ИТ-инфраструктура таких небольших компаний имеет крайне простую организацию, и все приложения,

включая business-critical, как правило, располагаются на одном IP-адресе. Иногда злоумышленнику достаточно просто зарегистрироваться на сайте, чтобы в заголовке ответного письма получить оригинальный IP-адрес и в дальнейшем его атаковать.
А поскольку на этом адресе находятся и «продающий» сайт для покупателей, и внутренний ресурс для партнеров ритейлера, то атака может полностью парализовать текущие бизнес-процессы. Срыв времени исполнения заказа или поставки оплаченного товара или услуг может привести к серьезным финансовым потерям, включая возмещение ущерба покупателю и контрагенту.

Исходя из публично доступных данных о выручке крупных игроков рынка, можно предположить, что их ущерб от DDoS-атак в среднем достигает 600 тыс. руб. в день. Для небольшого магазина этот показатель может составлять 50–100 тыс. руб. в день.

Иногда DDoS-атака может отвлекать ИБ-службу жертвы от более серьезного инцидента. Например, хакеры организуют самую простую DDoS-атаку и, пока ИБ-специалисты пытаются восстановить работоспособность сервера, крадут конфиденциальные данные покупателей, включая их имена, адреса, данные банковских карт.

Также DDoS-атака может быть связана с вымогательством: злоумышленники организуют «нападение» в критический для бизнеса момент (например, в сезон распродаж) и требуют деньги с жертвы в обмен на прекращение атаки. Хотя такой вариант развития событий встречается крайне редко. Намного чаще хакеры совершают показательную атаку, нарушив работу сайта на короткий период, и требуют деньги, чтобы предотвратить более серьезный сбой.

ВЫВОДЫ И ПРОГНОЗЫ

- За отчетный период количество DDoS-атак выросло в 2 раза, что стало результатом обострившейся конкурентной борьбы между игроками рынка на фоне увеличения спроса на услуги онлайн-магазинов.

- Пик атак пришелся на 4-й квартал года, когда большинство магазинов проводят акции вроде «Черной пятницы» и предновогодние распродажи.

- В основном злоумышленники использовали простые, но продолжительные атаки, которые не требовали долгой подготовки и больших финансовых затрат.

- Если в 2019 году атаки на ритейл были достаточно однотипны, а в 80% случаев применялся UDP flood, то в 2020 году техники хакеров стали разнообразнее (они задействовали все возможные амплификаторы, сократив долю UDP flood до четверти).

- Основной целью DDoS-атак на ритейл остается удар по репутации магазина и нанесение серьезного финансового вреда со стороны конкурентов, также подобная кибератака используется для вымогательства и отвлечения внимания ИБ-служб от более серьезных инцидентов.

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