DDoS-атаки в период COVID-19

сравнительная статистика за январь-май 2020 года

rt-solar.ru

Ростелеком
Солар

СОДЕРЖАНИЕ

Введение

Распространение COVID-19 и введение различных карантинных мер повлияло на все сферы жизни, поменяв наши привычки. Вынужденный перевод большинства активностей в онлайн-формат спровоцировал активность киберпреступников, которые увидели для себя новые возможности получения быстрой и легкой выгоды.

Эксперты «Ростелекома» подготовили отчет о том, как в этот сложный период поменялся ландшафт DDoS-атак на российские компании. Аналитика составлена на основе данных об атаках, наблюдаемых специалистами Центра кибербезопасности и защиты «Ростелекома» с января по май 2020 года.

ДЛЯ ОТЧЕТА БЫЛА ПРОАНАЛИЗИРОВАНА ИНФОРМАЦИЯ ПОЧТИ О 300 КОМПАНИЯХ ИЗ РАЗЛИЧНЫХ ОТРАСЛЕЙ, ВКЛЮЧАЯ ТЕЛЕКОМ, ГЕЙМИНГ, ОБРАЗОВАНИЕ, ФИНАНСОВЫЙ И ГОСУДАРСТВЕННЫЙ СЕКТОРА.

Основные тренды

В период действия карантина на фоне распространения COVID-19 (март–май 2020 года)

в 5 раз

выросло число DDoS-атак по сравнению с мартом–маем 2019 года

в 5,5 раз

выросло количество атак на образовательные ресурсы, а на госорганы и игровые серверы – примерно в 3 раза

150+ Гбит/с

составляла мощность большинства атак на операторов связи и дата-центы

36%

всех атак пришлось на апрель

ДОЛЯ ПРОСТЫХ И МАЛОМОЩНЫХ АТАК УВЕЛИЧИЛАСЬ. ЭТО УКАЗЫВАЕТ НА АКТИВНОСТЬ «НЕПРОФЕССИОНАЛЬНЫХ» ЗЛОУМЫШЛЕННИКОВ. В ОСНОВНОМ ОНИ ИСПОЛЬЗОВАЛИ ПРОСТЫЕ И ЛЕГКОДОСТУПНЫЕ ИНСТРУМЕНТЫ, НАПРИМЕР, ОБЫЧНУЮ DNS-АМПЛИФИКАЦИЮ ИЛИ NTP-АМПЛИФИКАЦИЮ.

КАК МЕНЯЛОСЬ КОЛИЧЕСТВО АТАК

В целом DDoS с каждым годом становится все популярнее у злоумышленников из-за простоты применения и низкой стоимости его организации. Неудивительно, что в период пандемии этот инструмент активно использовался злоумышленниками. В марте-мае 2020 года количество DDoS-атак, выявляемых экспертами «Ростелекома», увеличилось в 5 раз в сравнении с аналогичным периодом прошлого года. В целом за первые пять месяцев 2020 года общее число подобных атак год к году выросло более чем в 4 раза.

Отчетливо видно, как с начала года киберпреступники наращивали свою активность. Ее пик пришелся на апрель, когда количество атак в сравнении с январем увеличилось на 88%. Отметим, что годом ранее динамика не была такой яркой, а количество атак из месяца в месяц оставалось практически неизменным.

ПОДОБНЫЙ РЕЗКИЙ РОСТ DDOS СТАЛ СЛЕДСТВИЕМ РАСПРОСТРАНЕНИЯ COVID-19 В РОССИИ И МИРЕ.

Пандемия значительно повлияла на характер интернет-трафика, так как многие активности перешли в сеть. Вынужденное нахождение дома пользователи компенсировали активным обращением к онлайн-сервисам, и многие организации, чьи услуги ранее были представлены только в офлайн, запустили собственные интернет-ресурсы. Кроме того, работодатели были вынуждены перевести своих сотрудников на удаленную работу, и их рабочая деятельность также переместилась в сеть. Если раньше активность пользователей плавно нарастала в течение дня, достигая пика к вечеру, то теперь резкий рост отмечается с самого утра и не снижается до ночи. Соответственно вырос и объем передаваемого трафика, предоставив широкий простор для деятельности злоумышленников.

17:00-21:00 → 10:00-23:00

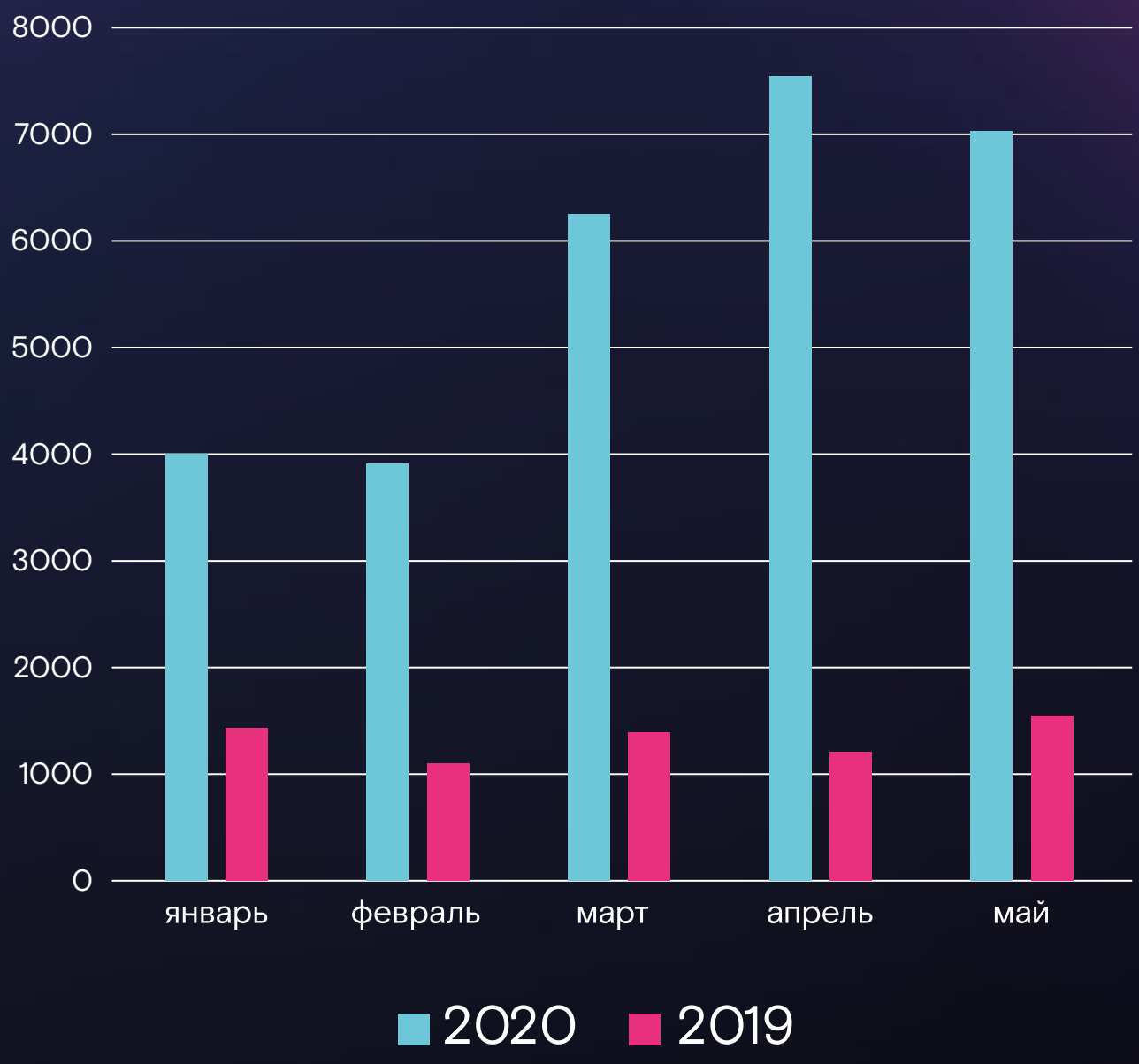
период активности пользователей до карантина

период активности пользователей во время карантина

20%

рост передаваемого трафика за март-май 2020

Количество атак за пять месяцев 2020 и 2019 года



ХАРАКТЕРИСТИКИ АТАК

При резком росте количества DDoS-атак их сложность и мощность в целом снизились. В основном злоумышленники использовали обычную DNS-амплификацию[1] или NTP-амплификацию[2] небольших объемов. Их простота заключается в том, что хакеры задействуют серверы, находящиеся в открытом доступе. Скорее всего, в отчетный период в большинстве атак применялись легкодоступные инструменты с уже устаревшим набором уязвимых серверов, что говорит о низкой квалификации злоумышленников.

Примечательно, что по итогам 2019 года эксперты «Ростелекома» фиксировали противоположный тренд: резкий рост мощности атак и их прогресс с технической точки зрения.

В период пандемии их количество не сократилось, но доля в целом упала на фоне резкого роста простых атак. Это еще раз указывает на то, что в отчетный период особенно активными в части DDoS были не «профессиональные» хакеры, а скорее «любители», которые решили воспользоваться ситуацией.

менее

3 Гбит/с

мощность большинства DDoS-атак в этот период

23 часа

продолжительность самой длинной атаки

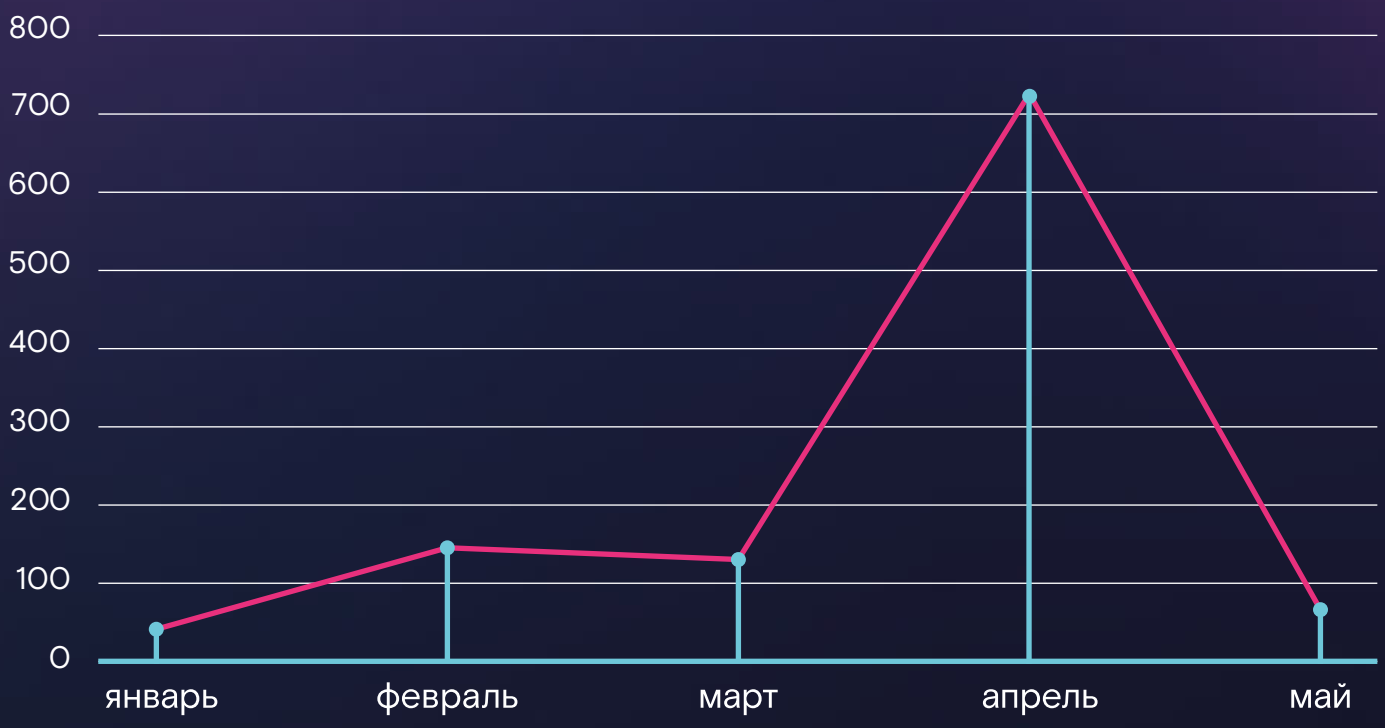
[1] *DNS-сервер хранит настройки каждого домена и обеспечивает связь между доменным именем и IP-адресом. При DNS-амплификации злоумышленник посылает запрос (обычно короткий) уязвимому DNS-серверу, который отвечает уже значительно большим по размеру пакетом. Если в качестве исходного IP стоит адрес компьютера жертвы (ip spoofing), то уязвимый DNS-сервер будет посылать в большом количестве ненужные пакеты компьютеру-жертве, пока полностью не парализует его работу.*

[2] *NTP-сервер – подключенный к интернету сервер точного времени, также поддерживающий службу мониторинга трафика. В ответ на команду «контрольный список» сервер отправляет список последних 600 подключенных к нему хостов. 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.*

ОСНОВНЫЕ ЖЕРТВЫ

В первые пять месяцев 2020 года резко вырос интерес хакеров к образовательным ресурсам (это в том числе различные электронные дневники, сайты с проверочными работами, площадки для онлайн-уроков и т.п). С марта по апрель количество атак на них увеличилось более чем в 5,5 раз.

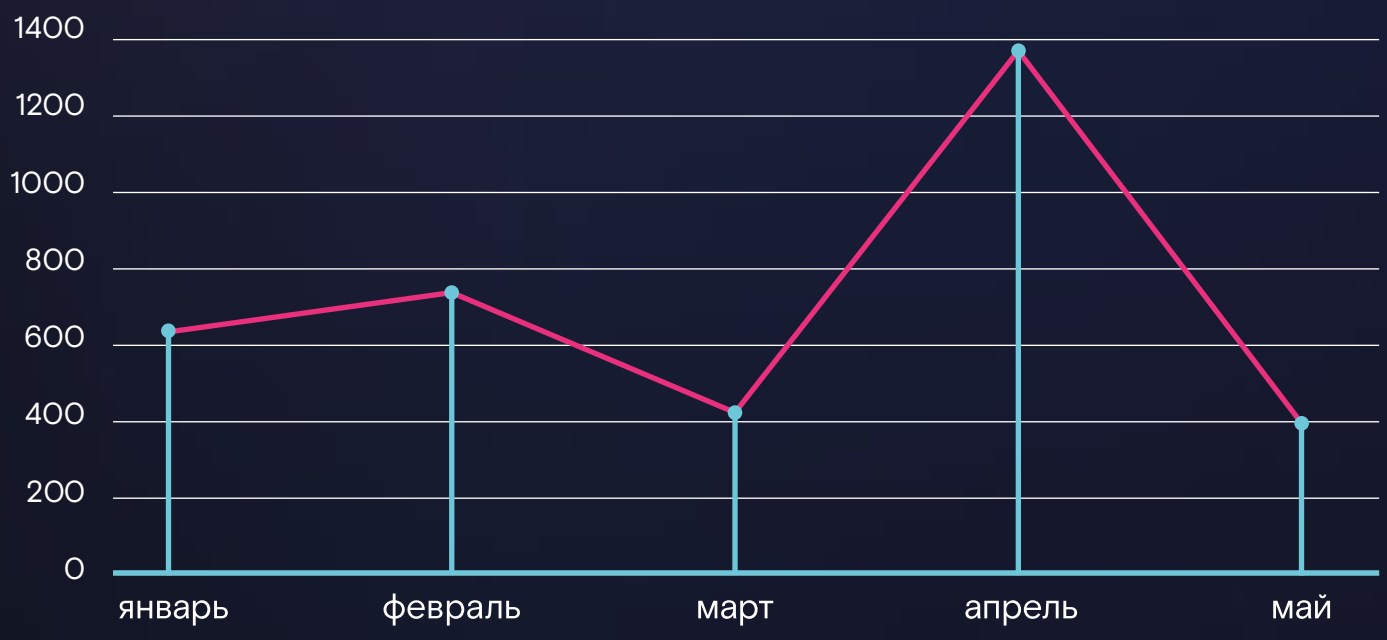
Динамика атак на образование за пять месяцев 2020 года



ЕСЛИ УЧЕСТЬ, ЧТО В БОЛЬШИНСТВЕ СЛУЧАЕВ «МУСОРНЫЙ» ТРАФИК ОТПРАВЛЯЛИ «ХАКЕРЫ-ЛЮБИТЕЛИ», МОЖНО ПРЕДПОЛОЖИТЬ, ЧТО В ЭТОМ СЛУЧАЕ ЗА DDOS СТОЯЛИ ШКОЛЬНИКИ, КОТОРЫЕ ХОТЕЛИ СДЕЛАТЬ НЕДОСТУПНЫМИ ДЛЯ СЕБЯ ЭЛЕКТРОННЫЕ КОНТРОЛЬНЫЕ, А ДЛЯ РОДИТЕЛЕЙ – СВОИ ДНЕВНИКИ.

Также наблюдалось значительное увеличение количества атак на государственные учреждения. В апреле, когда были оперативно запущены платформы для мониторинга передвижения граждан, услуги по выплате пособий и т.п., активность злоумышленников выросла более чем в 3 раза в сравнении с мартом того же года.

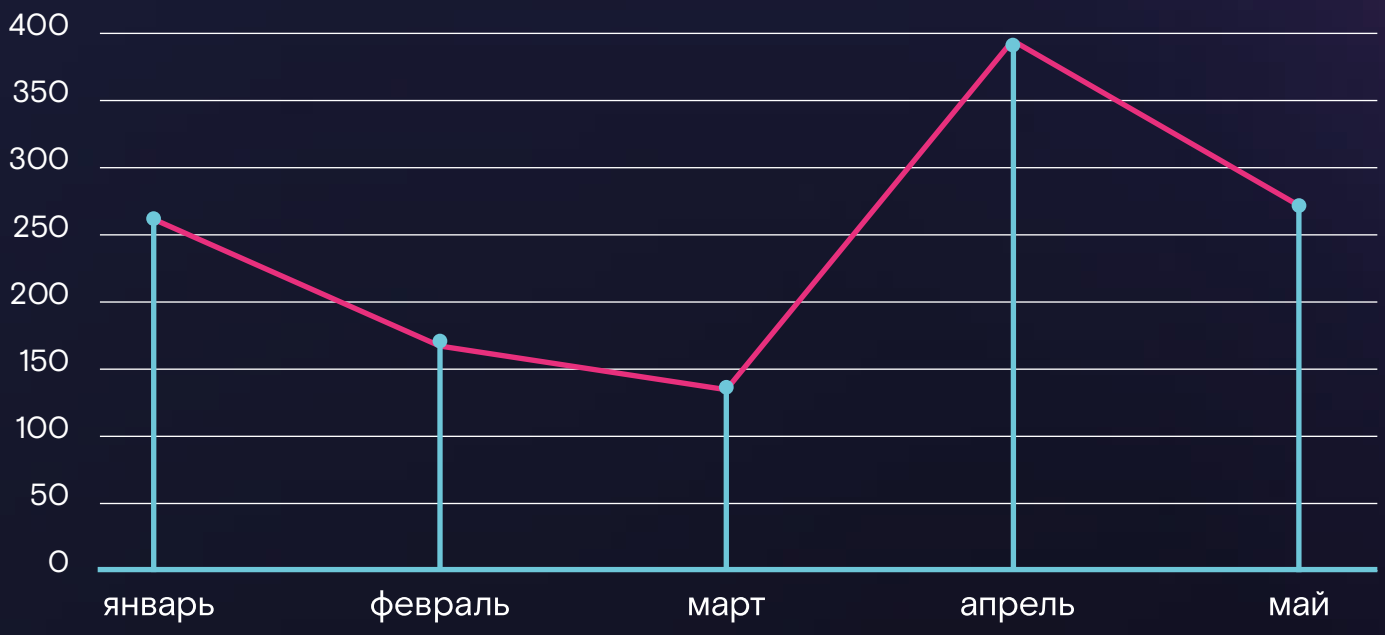
Динамика атак на госсектор за пять месяцев 2020 года



ВАЖНО ОТМЕТИТЬ, ЧТО РЕЧЬ ИДЕТ ИМЕННО ОБ АТАКАХ, А НЕ О РОСТЕ ЛЕГИТИМНОЙ НАГРУЗКИ НА ЭТИ РЕСУРСЫ, ТАК КАК СУЩЕСТВУЕТ МНОЖЕСТВО ФАКТОРОВ, ПОЗВОЛЯЮЩИХ ВЫДЕЛИТЬ «МУСОРНЫЙ» ТРАФИК И ОПРЕДЕЛИТЬ ФАКТ DDOS.

Третьей отраслью с наиболее выраженной динамикой стал игровой сегмент (рост атак в апреле почти в 3 раза в сравнении с мартом). Режим изоляции по всему миру значительно нарастил аудиторию онлайн-игр и киберспорта, который на время заменил зрителями реальные соревнования и чемпионаты. Эта индустрия смогла привлечь не только множество новых зрителей и пользователей, но и большой объем денежных средств, что обострило конкуренцию. Поэтому такой инструмент, как DDoS, позволяющий вывести из строя сайт конкурента, оказался очень востребован.

Динамика атак на игровой сегмент за пять месяцев 2020 года



ЕСЛИ В МАРТЕ НА ИГРОВЫЕ СЕРВЕРЫ БЫЛО СОВЕРШЕНО МЕНЕЕ 150 DDOS-АТАК, ТО В АПРЕЛЕ ЭТОТ ПОКАЗАТЕЛЬ ВЫРОС ПОЧТИ ДО 400.

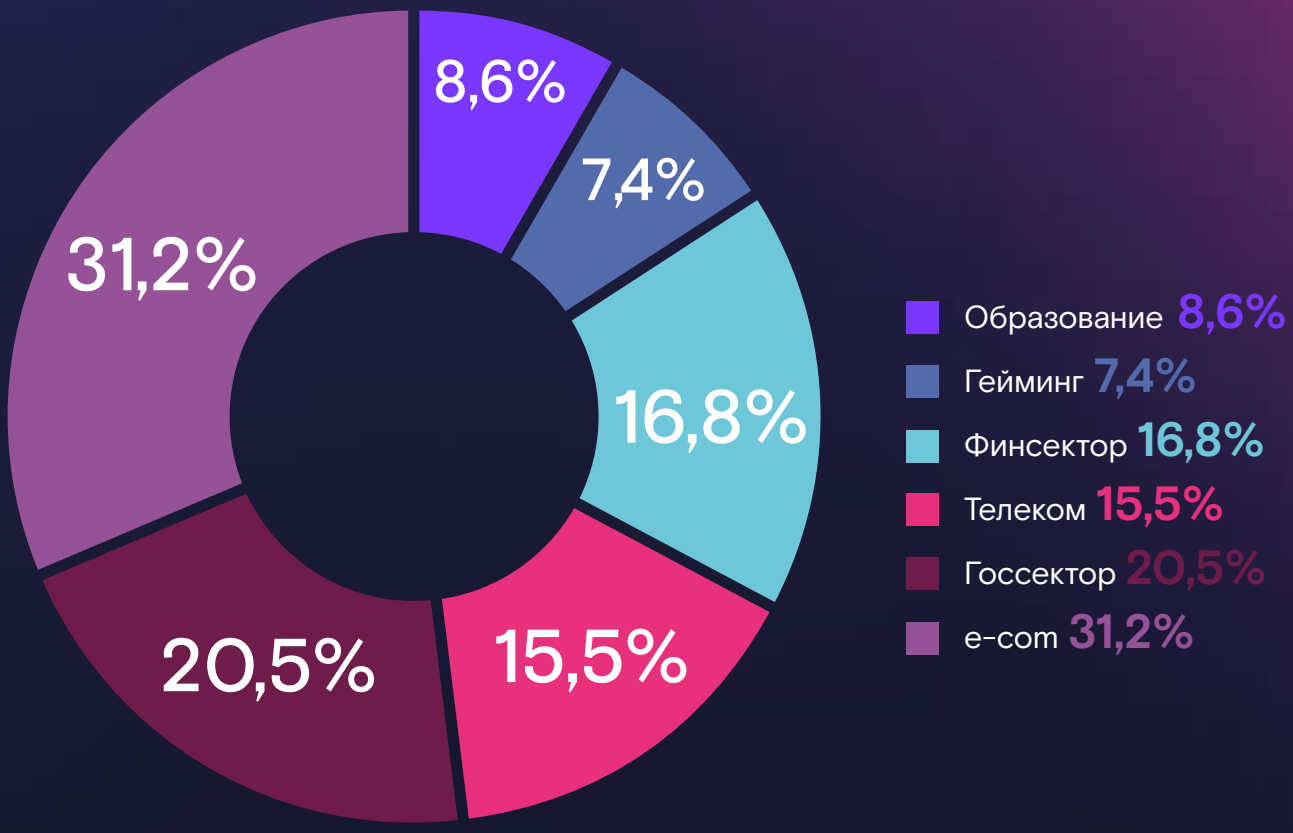
РАСПРЕДЕЛЕНИЕ DDOS-АТАК ПО ОТРАСЛЯМ

Несмотря на то, что в целом за отчетный период мощность атак упала, в общей статистике выделились операторы связи и дата-центры: здесь эксперты «Ростелекома» чаще обычного фиксировали атаки 150+Гбит/с. Такая активность злоумышленников связана с тем, что DDoS в этих двух сегментах позволяет вывести из строя не один конкретный сайт, а ударить «оптом» по клиентам оператора и ресурсам, которые обслуживает ЦОД. При этом такие компании более защищены и подготовлены к отражению киберугроз, чем, например, госучреждения или образовательный сегмент. Поэтому злоумышленникам приходится применять более совершенные инструменты, чтобы получить желаемый эффект. В период пандемии атаки на эти два сегмента были быстрыми и мощными и осуществлялись, скорее всего, через реальные хосты, собранные в одну бот-сеть. Это говорит об их технической зрелости и развитом механизме управления, позволяющем за считанные минуты перенаправить бот-сеть на новую жертву.

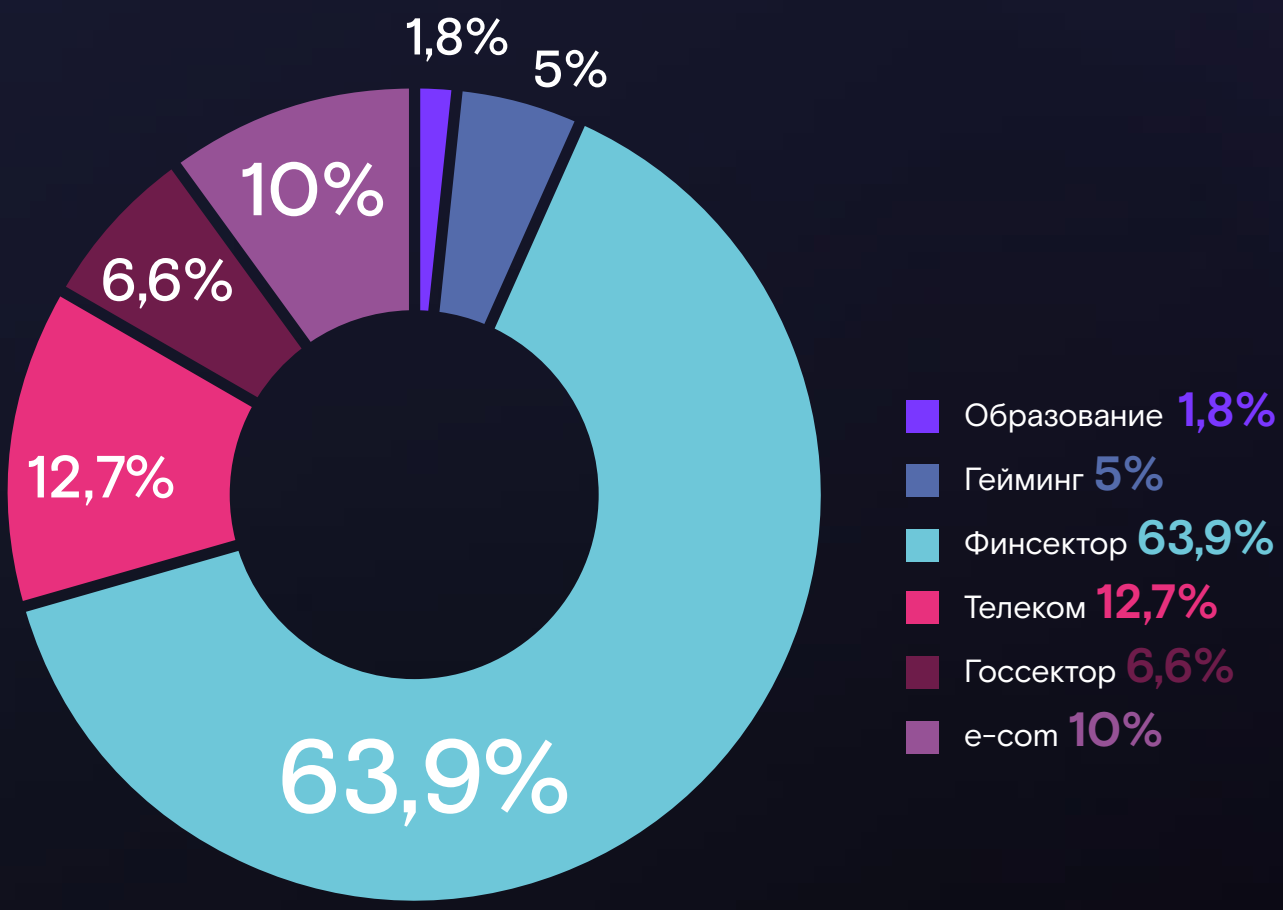
В целом такое разделение по отраслям продолжает тренд, который сформировался еще в 2019 году. Так, согласно более раннему исследованию «Ростелекома», в 2018 году на телеком-индустрию приходилось только 10% всех DDoS-атак, а в 2019 – уже 31%. Мишенями хакеров становились небольшие региональные интернет-провайдеры, хостинги и дата-центры, которые обычно не располагают необходимыми для отражения атак ресурсами.

> Также DDoS стал значительно чаще применяться в отношении образовательных учреждений и госструктур, что было связано с их активной цифровизацией и запуском собственных интернет-ресурсов.

Распределение DDoS-атак по отраслям март-май, 2020 год



Распределение DDoS-атак по отраслям март-май, 2019 год



Выводы

1. Организаторами DDoS в отчетный период чаще выступали «хакеры-любители», при этом количество «профессионалов» явно не уменьшилось.

2. Ключевыми жертвами стали сайты образовательных организаций и госструктур, на которые в период самоизоляции пришлась основная социальная нагрузка.

3. Игровой сегмент, будучи основным источником развлечения для сидящих дома граждан, также привлек внимание злоумышленников.

4. Из-за того, что в период карантина многие активности перешли в сеть, объем трафика в целом возрос примерно на 20%, а его профиль сильно изменился.

5. Теперь нагрузки на сеть, которые раньше достигали пика ближе к вечеру, резко возрастают к 10 утра и не снижаются до глубокой ночи, так как многие люди не ездят на работу и находятся у компьютера целый день.

6. В целом видно, что самым сложным для владельцев интернет-ресурсов месяцем стал апрель, когда в России действовал жесткий режим самоизоляции.

В мае активность хакеров постепенно начала спадать – этот тренд сохранится и дальше, если ситуация в России и мире будет стабилизироваться. Также можно прогнозировать сокращение количества атак на сектор образования после окончания периода вступительных и выпускных экзаменов.

Однако, как показал минувший карантин, спрогнозировать наверняка, когда компания столкнется с подобными атаками невозможно.

ПОЭТОМУ ЛУЧШЕ ЗАРАНЕЕ ПОДГОТОВИТЬСЯ К DDOS, ИНТЕГРИРОВАВ В СВОИ БИЗНЕС-ПРОЦЕССЫ СООТВЕТСТВУЮЩИЕ ИБ-РЕШЕНИЯ.

О КОМПАНИИ

«Ростелеком-Солар», компания группы ПАО «Ростелеком», — национальный провайдер сервисови технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью.

В основе подходов и технологий «Ростелеком-Солар» лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами защиты.

Задать вопрос или попробовать сервис
presale@rt-solar.ru

Ростелеком
Солар