SOLAR Rostelecom

Ростелеком

ОТЧЕТ О DDOS-АТАКАХ НА РОССИЙСКИЕ КОМПАНИИ В 2018 ГОДУ

МАРТ 2019

Основные тренды 2018 года:

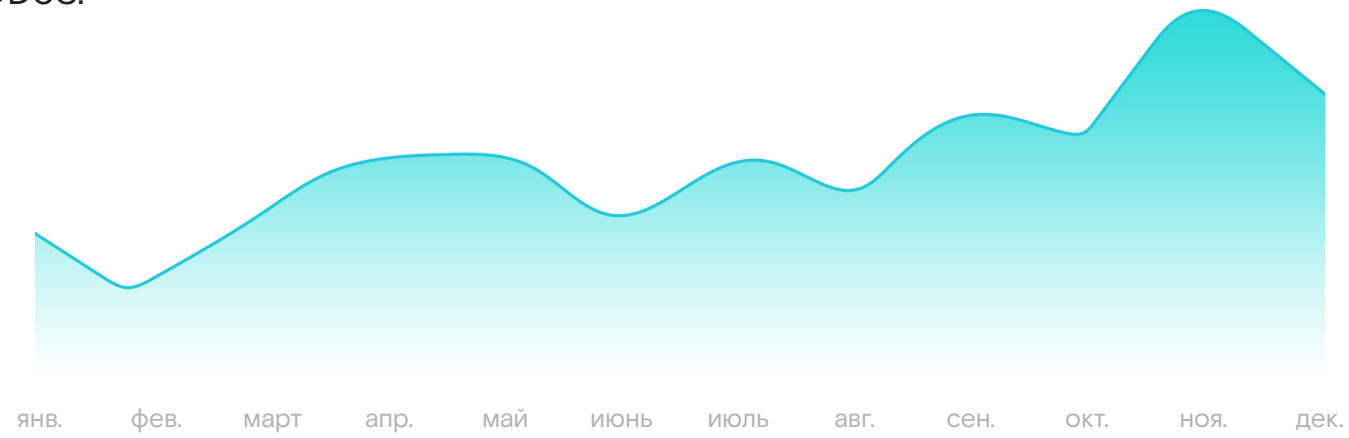
- **По сравнению с 2017** годом количество* DDoS-атак выросло почти в два раза – на 95%. На наш взгляд, во многом это связано с их дешевизной и эффективностью, которая будет способствовать кратному увеличению числа атак и в 2019 году.
- **Самая продолжительная атака**, зафиксированная «Ростелекомом» в 2018 году, продолжалась 280 часов (11 суток и 16 часов). Для сравнения, средняя DDoS-атака длится ~ 1.5-2 часа.
- **В ушедшем году** произошел резкий скачок мощности DDoS-атак. Самая сильная атака 2018 года велась с интенсивностью 450 Гбит/с, тогда как рекорд 2017 года – всего 54 Гбит/с.
- **Игровая индустрия** «лидирует» с большим отрывом: в 2017 году доля атак на эти компании составила 61%, в 2018 – 64%. По нашим прогнозам, данная картина не изменится в ближайшие годы, а с развитием киберспорта и появлением там еще больших денег можно ожидать дальнейшего роста числа атак на эту отрасль. Сфера электронной коммерции стабильно удерживает второе место (16%). Доля DDoS-атак на телеком выросла с 5% до 10%, а доля образовательных учреждений, напротив, резко сократилась – с 10% до 1%.
- **Рост среднего числа атак** на одного клиента составил 45% для игрового сегмента, 19% - для электронной коммерции.
- **Пик DDoS-атак** в 2018 году пришелся на ноябрь-декабрь. Эти месяцы считаются ключевыми с точки зрения продаж в сегменте электронной коммерции – покупательская активность растет в связи с предпраздничным периодом и стартом крупных распродаж. DDoS позволяет на время заблокировать ресурсы конкурента или может использоваться злоумышленниками в качестве орудия шантажа тех компаний, которые в ноябре-декабре получают большую часть выручки.
- **Наиболее популярным методом** DDoS является UDP-флуд – почти 38% всех атак осуществляется именно этим способом.
- **Отмечается резкий рост** доли атак с амплификацией и атак типа SYN-флуд. Их объединяет то, что первые не требуют наличия ботнета (и соответственно, затрат на его организацию/покупку), а вторые могут осуществляться как с использованием ботнета, так и без него.

* - здесь и далее приводятся данные о DDoS-атаках, наблюдаемых и нейтрализуемых на сети “Ростелеком”.

Распределение DDoS-атак по месяцам

Общее число DDoS атак в 2018 году увеличилось на 95% по сравнению с предыдущим годом. Наибольшее количество атак зафиксировано в ноябре и декабре.

Многие компании сегмента электронной коммерции получают существенную часть прибыли именно в праздники и предшествующие им недели – конкуренция в этот период особенно обостряется. Кроме того, на праздники приходится пик активности пользователей в онлайн-играх. Именно эти отрасли находятся в фокусе внимания злоумышленников, использующих в своих целях DDoS.



Длительность и мощность атак

Самая продолжительная атака, зафиксированная «Ростелекомом» в 2017 году, пришлась на август и продолжалась 263 часа (почти 11 суток). В 2018 году рекордных показателей достигла атака, зафиксированная в марте и продлившаяся 280 часов (11 суток и 16 часов).

В ушедшем году произошел резкий скачок мощности DDoS-атак. Если в 2017 году этот показатель не превышал 54 Гбит/с, то в 2018 самая серьезная атака велась уже со скоростью 450 Гбит/с. Это не было единичной флуктуацией. Лишь дважды за год этот показатель опускался существенно ниже 50 Гбит/с – в июне и августе.

Интенсивность DDoS-атак в 2018 г. (Гбит/с)

Самой мощной DDoS-атакой, обнаруженной и нейтрализованной «Ростелекомом», стала попытка злоумышленников повлиять на работу телеком-оператора Dtel.RU. Интенсивность атаки на пике составила 450 Гбит/с.

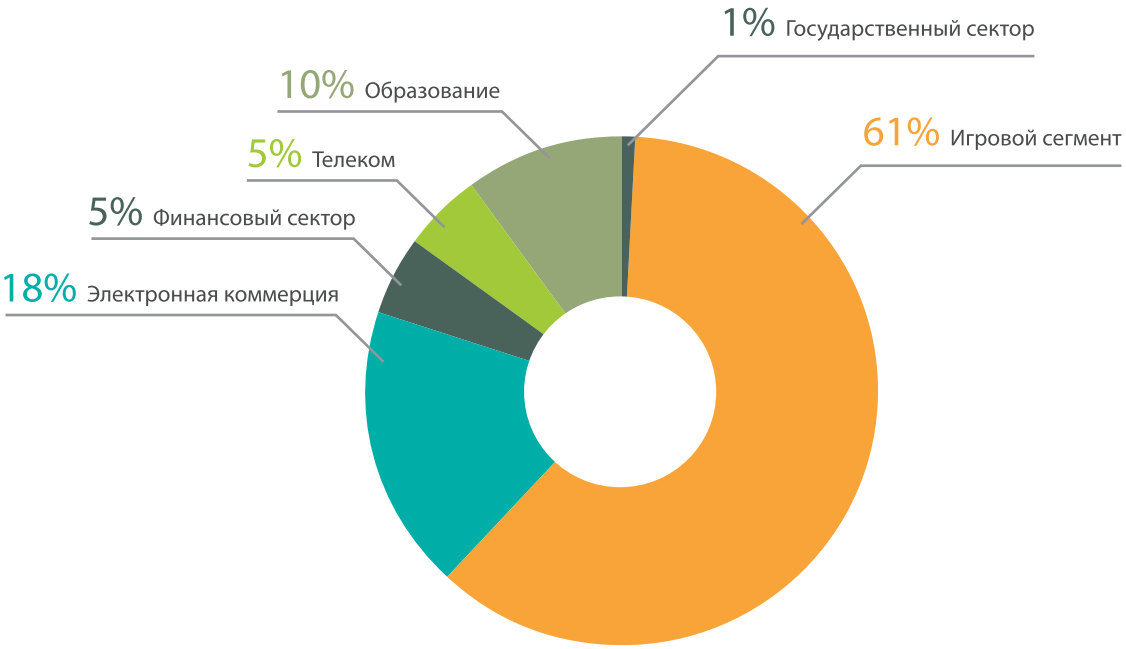
> **«Мы очень серьезно подходим к вопросам информационной безопасности, внимательно следим за появлением новых киберугроз и всегда стараемся обеспечить защиту заблаговременно. Эта стратегия доказывала свою эффективность уже не раз, так произошло и в данном случае. Несмотря на то, что атака была действительно очень сильной, все интернет-сервисы функционировали в штатном режиме, и действия киберпреступников никак не затронули наших абонентов».**
>
> Сергей Мелешко
> старший администратор сети компании Dtel.RU

В среднем атака мощностью более 30-50 Гбит/с уже является серьезным испытанием. Говорить о самостоятельной защите от подобных атак не приходится, это практически невозможно без потери легитимного трафика конечных пользователей защищаемого ресурса. Атака в 450 Гбит/с с большой вероятностью «положила» бы сеть практически любого регионального оператора. Такая слабая устойчивость к DDoS связана с низким уровнем проникновения сервиса в регионах, а также недостаточной эффективностью облачных сервисов Anti-DDoS.

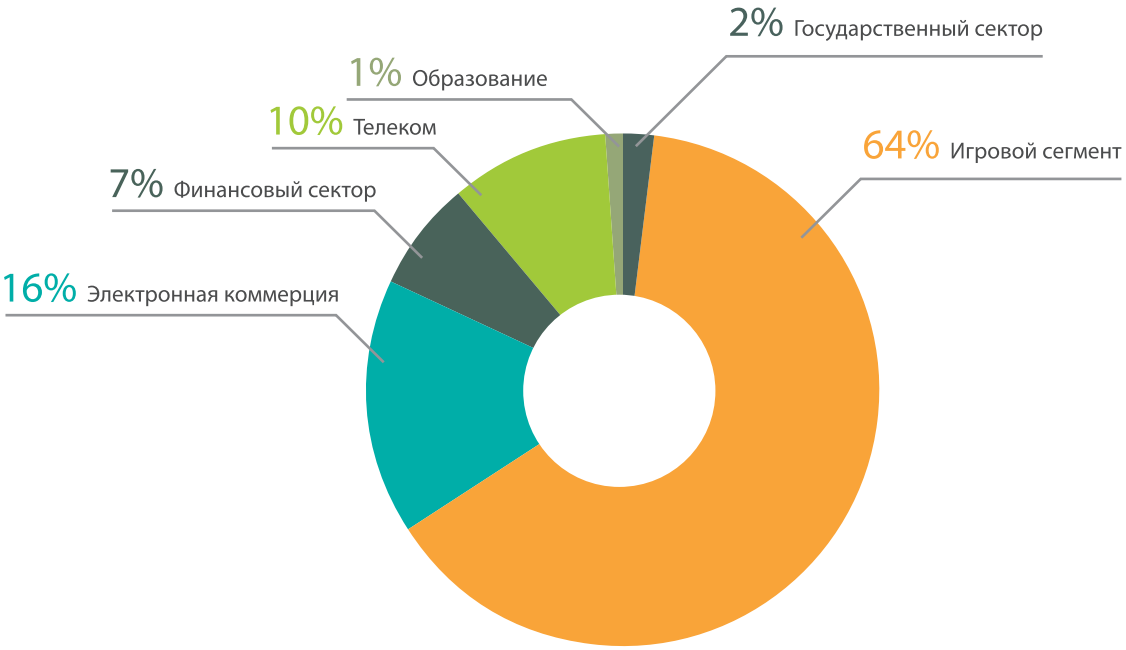
Распределение DDoS-атак по отраслям

Статистика 2018 года подтверждает, что угроза DDoS наиболее актуальна для отраслей, чьи критически важные бизнес-процессы зависят от доступности онлайн-сервисов и приложений – в первую очередь, это игровой сегмент и электронная коммерция.

Распределение DDoS-атак по отраслям, 2017 год

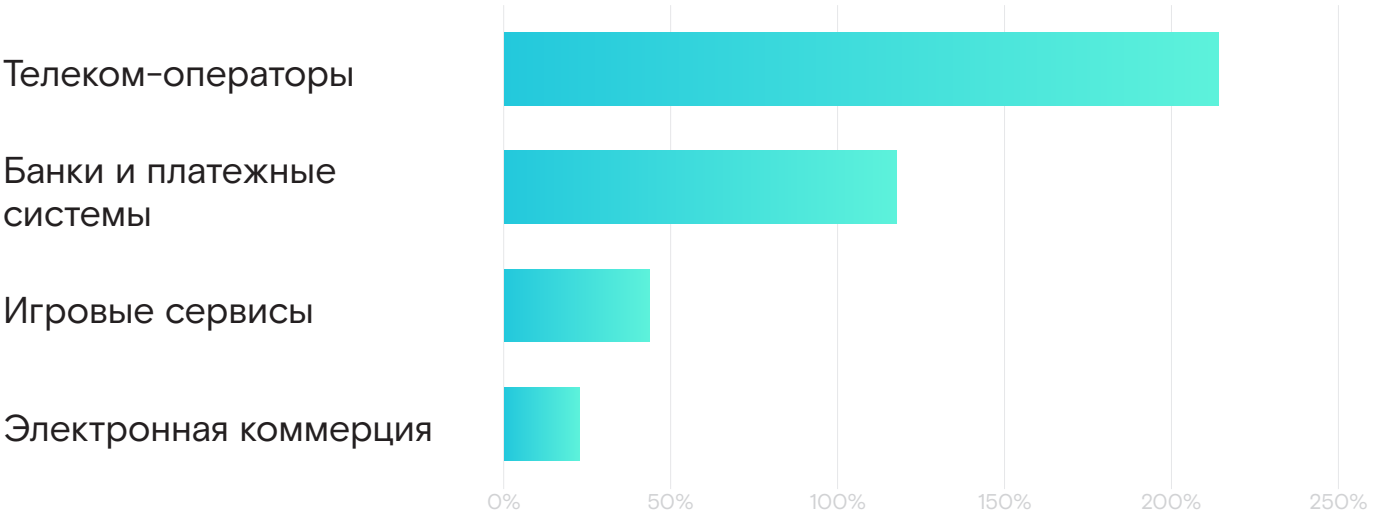


Распределение DDoS-атак по отраслям, 2018 год



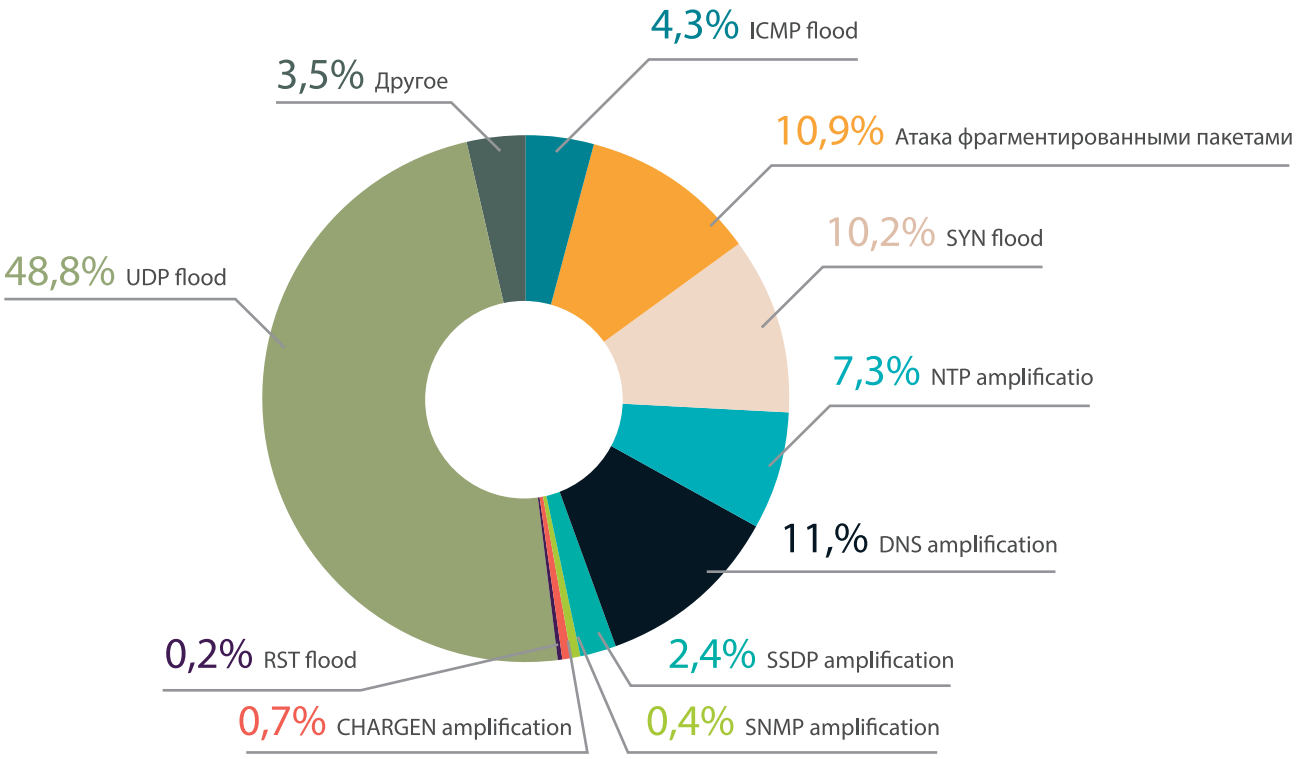
Игровая индустрия «лидирует» с большим отрывом: в 2017 году доля атак на эти компании составила 61%, в 2018 – 64%. По нашим прогнозам, данная картина не изменится в ближайшие годы, а с развитием киберспорта и появлением там еще больших денег можно ожидать дальнейшего роста числа атак на эту отрасль. Сфера электронной коммерции стабильно удерживает второе место (16%). Доля DDoS-атак на телеком выросла с 5% до 10%, а доля образовательных учреждений, напротив, резко сократилась – с 10% до 1%.

Рост числа атак на одного клиента

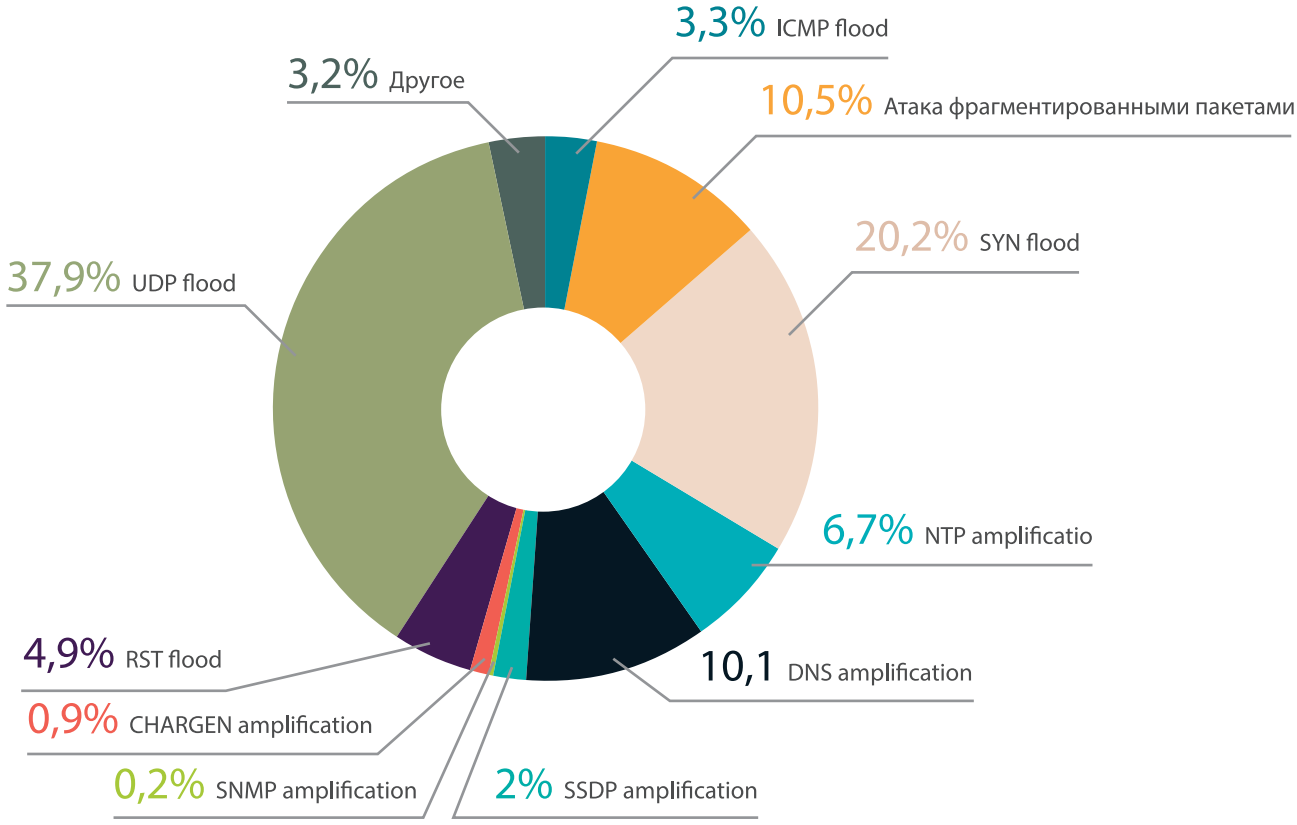


Предсказуемой тенденцией является наблюдаемый рост среднего числа атак на одного клиента из игрового сегмента (45%) и электронной коммерции (19%). При этом некоторым сюрпризом стал значительный рост атак на банки и платежные системы. Но это объясняется скорее очень спокойным 2017 годом после кампании против российского банковского сектора в конце 2016. В 2018 году все «вернулось на свои места», и в 2019 мы ожидаем дальнейшего роста атак на эту отрасль.

Распределение DDoS-атак по типам, 2017 год



Распределение DDoS-атак по типам, 2018 год



Наиболее популярным методом DDoS является UDP-флуд – почти 38% всех атак осуществляется именно этим способом. За ним следует SYN-флуд (20,2%) и почти в равных долях атака фрагментированными пакетами и DNS-амплификация – 10,5% и 10,1% соответственно.

При этом сравнение статистики за 2017 и 2018 гг. показывает, что доля атак типа SYN-флуд выросла почти в два раза. Мы предполагаем, что это связано с относительной простотой и дешевизной атак этого типа, т.к. они не требуют обязательного наличия ботнета. SYN-флуд представляет собой трафик с подделанными адресами источников, его можно запустить с любого сервера с широкими каналами. Порой увеличение SYN-пакетов – признак прикладных атак. Как правило, они находятся на стыке технологий, и их фильтрация должна осуществляться, в том числе, с применением технологий WAF (Web Application Firewall).

Также мы отмечаем рост числа атак с использованием амплификаторов. При организации DDoS с амплификацией злоумышленники отправляют запросыс поддельным адресом источника к серверам, которые отвечают жертве атаки многократно увеличенными пакетами. Такой способ DDoS-атак может выйти на новый виток и стать очень распространенным уже в ближайшее время, поскольку он также не требует затрат на организацию или покупку ботнета. В этой связи крупные операторы наряду с защитой безопасности конечных устройств должны обеспечить особое внимание уязвимым серверам амплификации в собственной сети.

С другой стороны, с развитием интернета вещей и ростом числа известных уязвимостей IoT-устройств можно ожидать появления и новых мощных ботнетов, а следовательно – и удешевления услуг по организации DDoS-атак.

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