DDoS-атаки 2019 – начало 2020

Выводы и прогнозы

rt-solar.ru

Ростелеком
Солар

СОДЕРЖАНИЕ

Основные тренды

Возросло количество мощных атак

63%

Рост количества атак относительно 2018 года

153%

Рост среднего числа атак на одного клиента в сфере образования

Злоумышленники стали активнее использовать устройства Интернета вещей

Продолжительность атак резко снизилась

Наибольший риск быть атакованными сохраняется за игровой индустрией

Злоумышленники экспериментируют с векторами атак и их комбинациями

3 000 целей

Самая распределенная атака

8 000 устройств

Самый большой выявленный ботнет

UDP flood

Наиболее популярный метод DDoS-атак

WSD ARMS

Новые освоенные злоумышленниками амплификаторы

Здесь и далее приводятся данные о DDoS-атаках, наблюдаемых и нейтрализуемых в сети «Ростелеком»

Главные наблюдения

ПО МНЕНИЮ ЭКСПЕРТОВ «РОСТЕЛЕКОМ-СОЛАР», С РАЗВИТИЕМ ПОКОЛЕНИЯ СВЯЗИ 5G ПРОБЛЕМА ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЬСКИХ УСТРОЙСТВ СТАНЕТ ЕЩЕ БОЛЕЕ АКТУАЛЬНОЙ, ЧТО НАВЕРНЯКА ПРИВЕДЕТ К НОВЫМ ВСПЛЕСКАМ DDOS-АТАК

ИСПОЛЬЗОВАНИЕ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

Устройства Интернета вещей (IoT) стали активно использоваться для проведения DDoS-атак, что неоднократно отмечали эксперты «Ростелеком-Солар» на протяжении всего отчетного периода. Так, была зафиксирована атака типа SYN flood на букмекерскую компанию, рекордная по мощности для сети «Ростелекома» — 178 Mpps (миллионов пакетов в секунду). Злоумышленники использовали бот-сеть из 8 000 реальных устройств: домашних роутеров, камер и прочих устройств Интернета вещей, а также мобильных телефонов.

В сентябре 2019 года из-за атаки с помощью IoT-устройств пользователи во всем мире столкнулись с недоступностью Википедии и Twitch[1].

По мнению экспертов «Ростелеком-Солар», с развитием поколения связи 5G проблема защищенности пользовательских устройств станет еще более актуальной, что наверняка приведет к новым всплескам DDoS-атак.

1 https://www.cnews.ru/news/top/2019-09-11_ddosatakaulozhivshaya_na_vikipediyu

НОВЫЕ МОЩНЫЕ АМПЛИФИКАТОРЫ

В 2019 году злоумышленники открыли потенциал UDP-based протокола Apple Remote Desktop (UDP-порт 3283), фактор амплификации[2] которого согласно исследованию Netscout составляет 35.5:1. Apple Remote Desktop — приложение удаленного администрирования рабочих станций под управлением macOS.

К указанному ранее UDP-порту обращается служба ARMS (Apple's Remote Management Service). Данный порт постоянно открыт на станциях под управлением macOS, если включен режим Remote Management, даже если это противоречит настройкам безопасности на файрволе.

В июне 2019 года было выявлено около 54 000 доступных из интернета компьютеров с включенной службой ARMS. Большая их часть располагалась в кампусах университетов США. На данный момент во многом благодаря оперативной реакции университетов количество таких устройств снизилось.

2 DDoS-амплификация – процесс, при котором публичному интернет-сервису (например, NTP) направляется относительно короткий запрос с поддельным адресом источника. Сервер амплификации отвечает в адрес жертвы многократно увеличенным ответом по сравнению с длиной запроса

Тем не менее на сегодня фиксируется более 16 000 компьютеров под управлением macOS с открытым UDP-портом. Злоумышленнику остается лишь найти любые из них и использовать для проведения и усиления атаки. В 2019 – начале 2020 года на сетях «Ростелекома» наблюдалось множество атак данного типа.

> Также злоумышленники активно используют протокол обнаружения устройств WS-Discovery (Web Services Dynamic Discovery). По данным Netscout, фактор его амплификации составляет 500:1.

Протокол используется устройствами Интернета вещей. Как и Apple Remote Desktop, WS-Discovery использует UDP-based протокол для передачи пакетов, что позволяет злоумышленникам применять спуфинг (то есть подмену IP-адреса) назначения пакетов. Согласно данным BinaryEdge, в сентябре 2019 года в интернете насчитывалось порядка 630 000 устройств с данной уязвимостью.

«КОВРОВЫЕ БОМБАРДИРОВКИ»

Среди необычных атак прошлого года можно отметить так называемые «ковровые бомбардировки». Для данного типа характерен перебор целей в адресном пространстве атакуемого в поиске наиболее уязвимой. Это усложняет обнаружение и противодействие атакам в модели защиты per IP, когда под защиту ставятся лишь отдельные IP-адреса, а не вся интернет-инфраструктура. Самая массивная из зафиксированных нами «ковровых бомбардировок» включала почти 3000 целей — был перепробован каждый адрес всех сетей одного клиента.

САМАЯ МАССИВНАЯ ИЗ ЗАФИКСИРОВАННЫХ НАМИ «КОВРОВЫХ БОМБАРДИРОВОК» ВКЛЮЧАЛА ПОЧТИ 3000 ЦЕЛЕЙ — БЫЛ ПЕРЕПРОБОВАН КАЖДЫЙ АДРЕС ВСЕХ СЕТЕЙ ОДНОГО КЛИЕНТА

16 000
Компьютеров, уязвимых к амплификации ARMS

630 000
Устройств, уязвимых к амплификации WSD

35.5:1
Фактор амплификации ARMS

500:1
Фактор амплификации WSD

178 Mpps
Атака типа SYN flood, рекордная по мощности для сети «Ростелекома»

8 000 устройств
Использованная злоумышленниками бот-сеть

Википедия и Twitch
Широко известные жертвы DDoS-атак с использованием IoT-устройств

РАСПРЕДЕЛЕНИЕ DDOS-АТАК ПО МЕСЯЦАМ

По сравнению с 2018 годом количество DDoS-атак, как и прогнозировали эксперты «Ростелеком-Солар», выросло более чем в 1,5 раза — на 63%. Таким образом, закрытие ряда значимых так называемых стрессеров, а по факту сервисов организации DDoS (Quantum Stresser[3], ExoStress.in, QuezStresser.com и пр.[4]), почти не оказало влияния на теневую сферу DDoS-услуг. Организация таких атак — это по-прежнему дешево и достаточно просто.

> Пик DDoS-атак в 2019 году пришелся на октябрь. Это связано с подготовкой представителей электронной коммерции к Черной пятнице — уже с середины октября проводились различные акции, предшествующие главной распродаже. Именно на представителей электронной коммерции пришлось наибольшее количество атак в этот период.

При этом крупных игроков данного сегмента в основном атакуют не с помощью стрессеров, а используя многовекторные целевые атаки, так как в области большого бизнеса злоумышленники стараются действовать наверняка.

ПИК DDOS-АТАК В 2019 ГОДУ ПРИШЕЛСЯ НА ОКТЯБРЬ. ЭТО СВЯЗАНО С ПОДГОТОВКОЙ ПРЕДСТАВИТЕЛЕЙ ЭЛЕКТРОННОЙ КОММЕРЦИИ К ЧЕРНОЙ ПЯТНИЦЕ

23 часа 40 минут

Самая продолжительная атака 2019 года

11 суток 16 часов

Самая продолжительная атака 2018 года

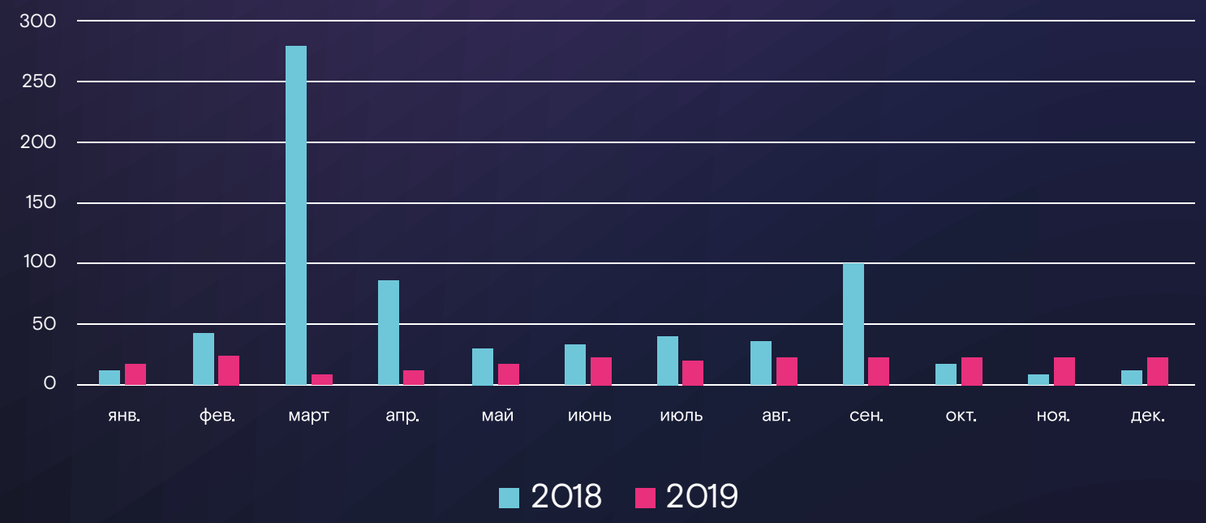
3 https://www.cnews.ru/news/top/2020-02-07_izvestnyj_haker_skryvalsya

4 https://xakep.ru/2019/11/19/exostresser-sentenced/

ДЛИТЕЛЬНОСТЬ И МОЩНОСТЬ АТАК

Продолжительность DDoS-атак резко снизилась по сравнению с предыдущим годом. Так, самая продолжительная атака в 2019 году длилась около суток, в то время как в 2018 году — 11 суток и 16 часов.

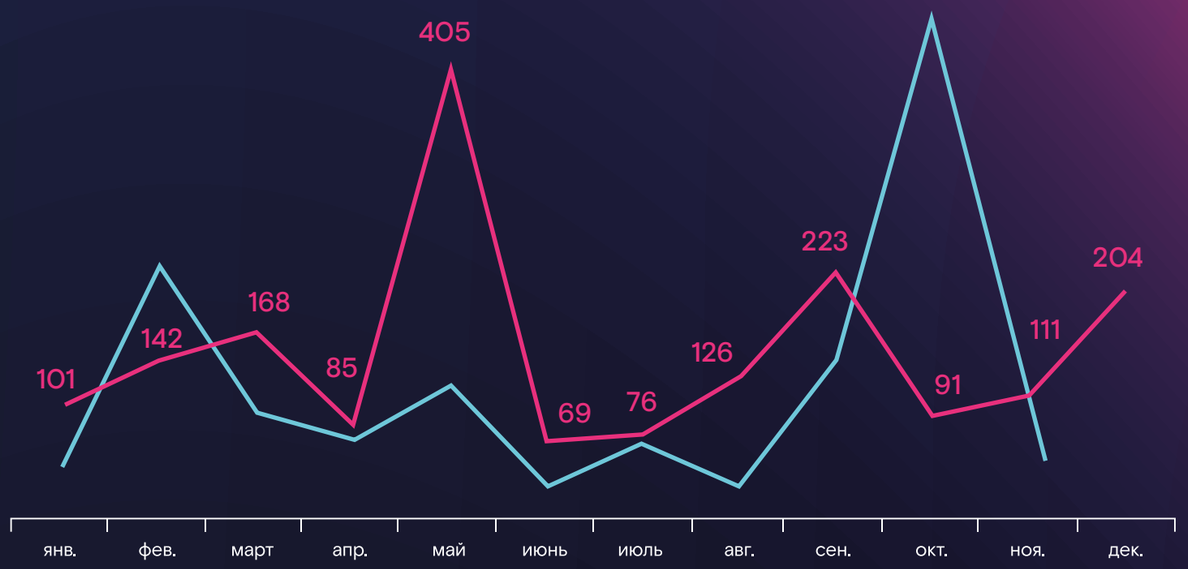
Сравнение продолжительности DDoS-атак, часы



В ПРОТИВОВЕС ПРОДОЛЖИТЕЛЬНОСТИ ВОЗРОСЛО КОЛИЧЕСТВО МОЩНЫХ DDOS-АТАК. НОВОГО РЕКОРДА НЕ СЛУЧИЛОСЬ — САМАЯ МОЩНАЯ DDOS-АТАКА 2019 ГОДА ВЕЛАСЬ С ИНТЕНСИВНОСТЬЮ В 405 ГБИТ/С, ЧТО НЕСКОЛЬКО МЕНЬШЕ, ЧЕМ В 2018 ГОДУ — 450 ГБИТ/С. ОДНАКО В СРЕДНЕМ ПОКАЗАТЕЛИ МОЩНОСТИ DDOS БЫЛИ ВЫШЕ, ЧЕМ В 2018 ГОДУ

ТРЕНД 2019 ГОДА: ЗЛОУМЫШЛЕННИКИ НЕ ВЫМАТЫВАЛИ ЖЕРТВУ ПРОДОЛЖИТЕЛЬНЫМИ МАЛОМОЩНЫМИ АТАКАМИ, А ПРОВОДИЛИ СПРИНТЫ СО ВЗРЫВАМИ ПАРАЗИТНОГО ТРАФИКА

Сравнение интенсивности DDoS-атак, Гбит/с



Таким образом, трендом 2019 года стало то, что злоумышленники не выматывали жертву продолжительными маломощными атаками, а проводили спринты со взрывами паразитного трафика. Этот тренд может объясняться тем, что в ходе атаки ботнеты, которые являются ценным активом для хакеров, могут быть раскрыты защитниками.

После нейтрализации атаки данные об адресах ботнетов поступают другим операторам в рамках различных информационных обменов. В этом случае ботнет становится непригоден. Если же быстро атаковать жертву мощной волной запросов, то сервис Anti-DDoS не успевает наполнить черный список.

РАСПРЕДЕЛЕНИЕ DDOS-АТАК ПО ОТРАСЛЯМ

Поскольку это исследование базируется на данных об атаках на заказчиков сервиса Anti-DDoS компании «Ростелеком», при определении наиболее атакуемых отраслей мы формируем два аналитических среза:

1. Простое распределение общего числа зафиксированных атак по отраслям.
2. Средний рост числа атак на одного клиента отрасли. Этот показатель нивелирует возможность погрешности, связанной с увеличением количества заказчиков из определенной отрасли и, как следствие, увеличением числа атак, которые фиксирует сервис.

ОБЩЕЕ РАСПРЕДЕЛЕНИЕ DDOS-АТАК ПО ОТРАСЛЯМ

В целом по отраслям распределение получилось более равномерным, чем в 2018 и 2017 годах. Игровая индустрия по-прежнему лидирует: на нее пришлось 34% от общего числа атак (против 64% в 2018 году). Однако с учетом активного развития киберспорта ожидать дальнейшего снижения количества атак на этот сегмент не приходится.

Сложность фильтрации таких атак в том, что игровые протоколы используют UDP в качестве транспорта. Это позволяет подменять адреса отправителя и затрудняет отслеживание сессий.

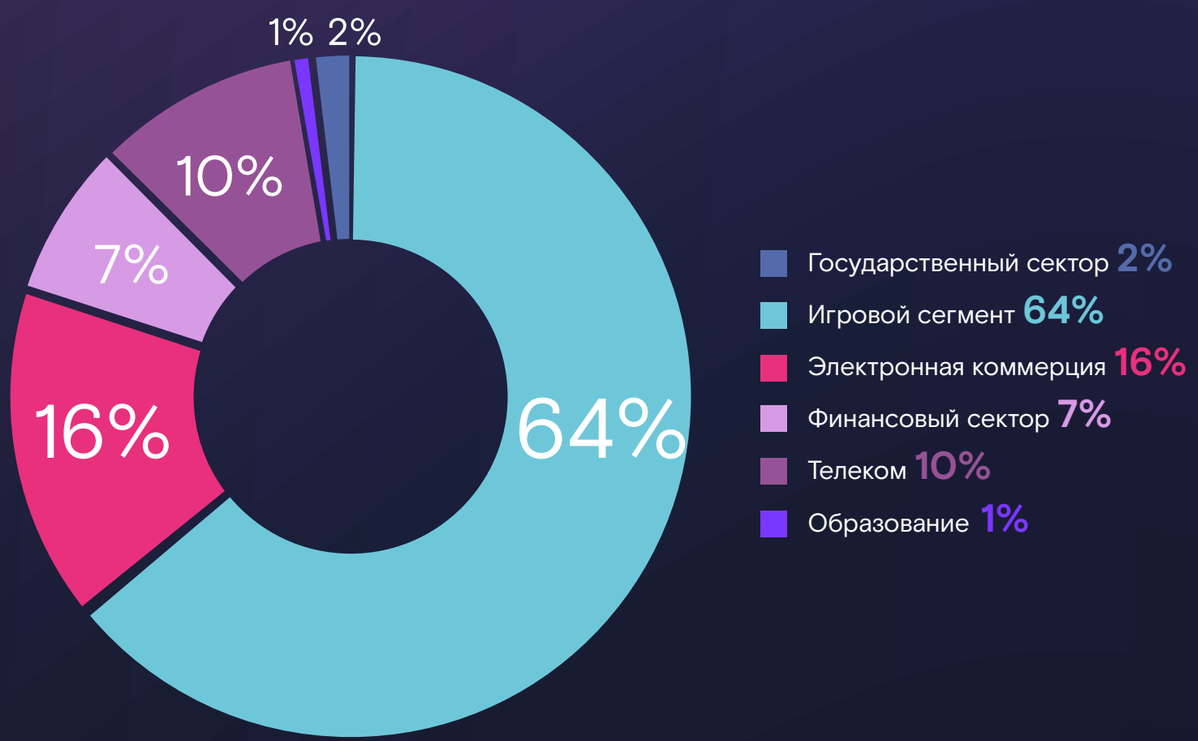
В 2019 году можно выделить два типа DDoS-атак уровня приложений на игровые серверы. Первый добивается их недоступности путем отправки большого количества пакетов, которые для стороннего сервиса защиты похожи на легитимные. Защита от таких атак основана на профилировании легитимного трафика и таких мерах, как regexp[5] и challenge-response[6].

Второй тип связан с эксплуатацией выявленных уязвимостей игровых протоколов и платформ. В данном случае для проактивной защиты необходим другой класс устройств — Game application firewall. Отдельные меры сейчас принимаются крупными игровыми хостингами и производителями, которые встраивают различные проверки в свои программы-клиенты и связывают их с самостоятельно разработанными системами защиты.

5 Regexp контрмеры основаны на поиске в содержимом пакета определенной подстроки, описанной специальным синтаксисом — регулярным выражением

6 Challenge-response меры — проверка подлинности пользователя игрового сервиса на основании определенного алгоритма аутентификации программы-клиента на сервере

Распределение DDoS-атак по отраслям, 2018 год



Распределение DDoS-атак по отраслям, 2019 год

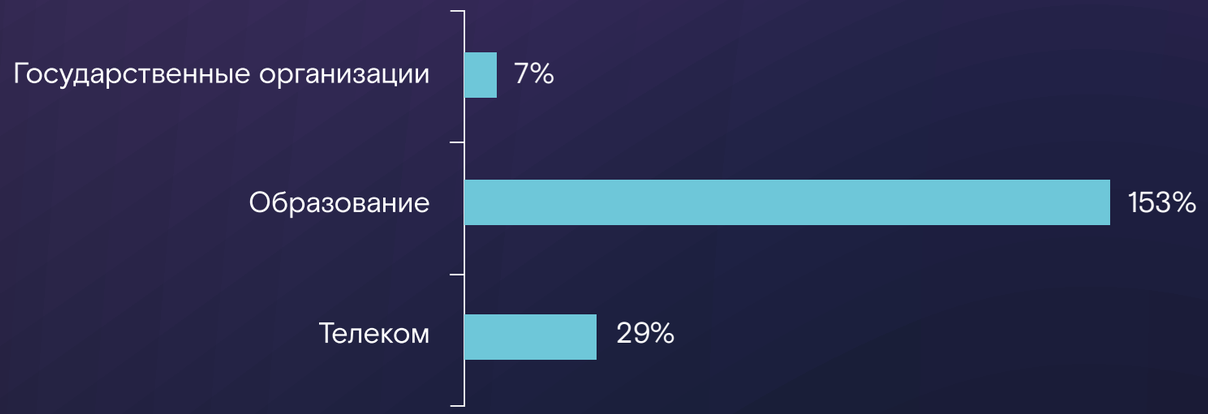
Значительно увеличилась доля атак на представителей телекома — как правило, это некрупные региональные ISP, различные хостинги и дата-центры. Для злоумышленников они являются достаточно легкой целью, так как обычно не располагают необходимыми для отражения мощных DDoS-атак ресурсами, не считая тех случаев, когда находятся под защитой своих аплинков — магистральных операторов.

В финансовом секторе без изменений — доля атак составляет все те же 7%, что и в 2018 году. А вот доля атак на образовательные учреждения и государственный сектор увеличилась, что вполне прогнозируемо с учетом все большего распространения онлайн-составляющей в данных сегментах. Кроме того, в 2019 году «Ростелеком» отразил ряд мощных атак на крупные банки и несколько мероприятий федерального масштаба.

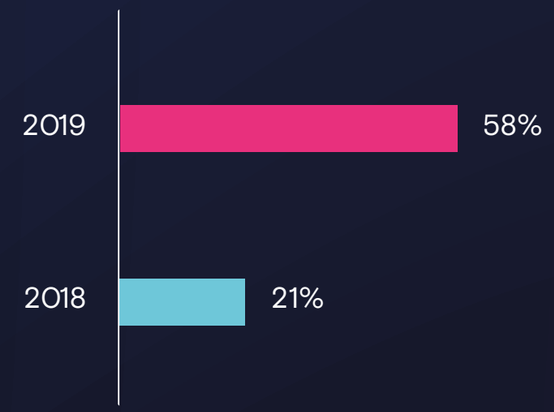
РОСТ ЧИСЛА АТАК НА ОДНОГО КЛИЕНТА

Наибольший рост числа атак в расчете на одного клиента показали образовательные учреждения, в том числе различные электронные дневники, экзаменационные ресурсы и тому подобное.
Как уже было сказано ранее, связано это с тем, что деятельность представителей данного сегмента все больше зависит от доступности онлайн-ресурсов, особенно в период самоизоляции.

Есть основания полагать, что инициаторами таких атак служат сами учащиеся, что еще раз демонстрирует, насколько доступной стала организация DDoS-атак. При этом на сегодняшний день образовательные учреждения защищены относительно слабо, поэтому остановить работу их онлайн-ресурсов может даже базовая DDoS-атака.



Если сравнивать 2018 и 2019 годы, то средний рост количества атак в расчете на одного клиента по всем сегментам составил 21% и 58% соответственно.



РАСПРЕДЕЛЕНИЕ DDOS-АТАК ПО ТИПАМ

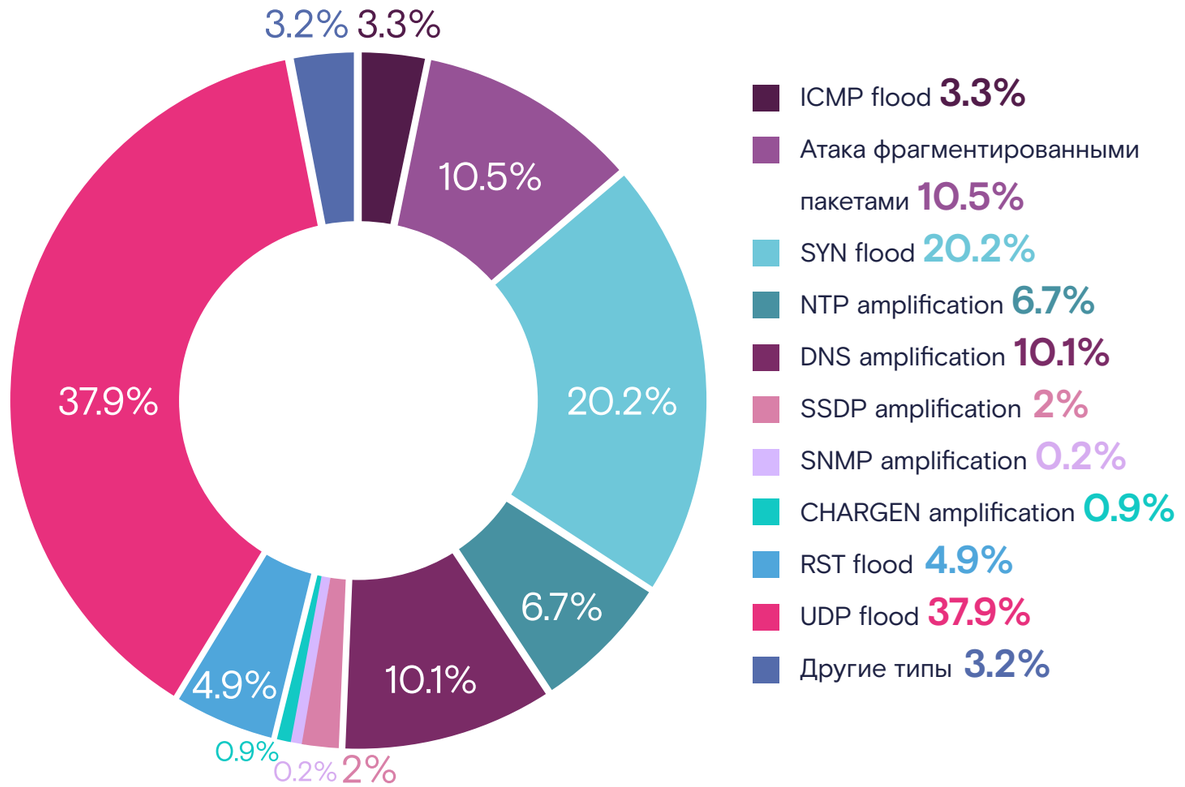
31.5%
UDP flood

27.4%
SYN flood

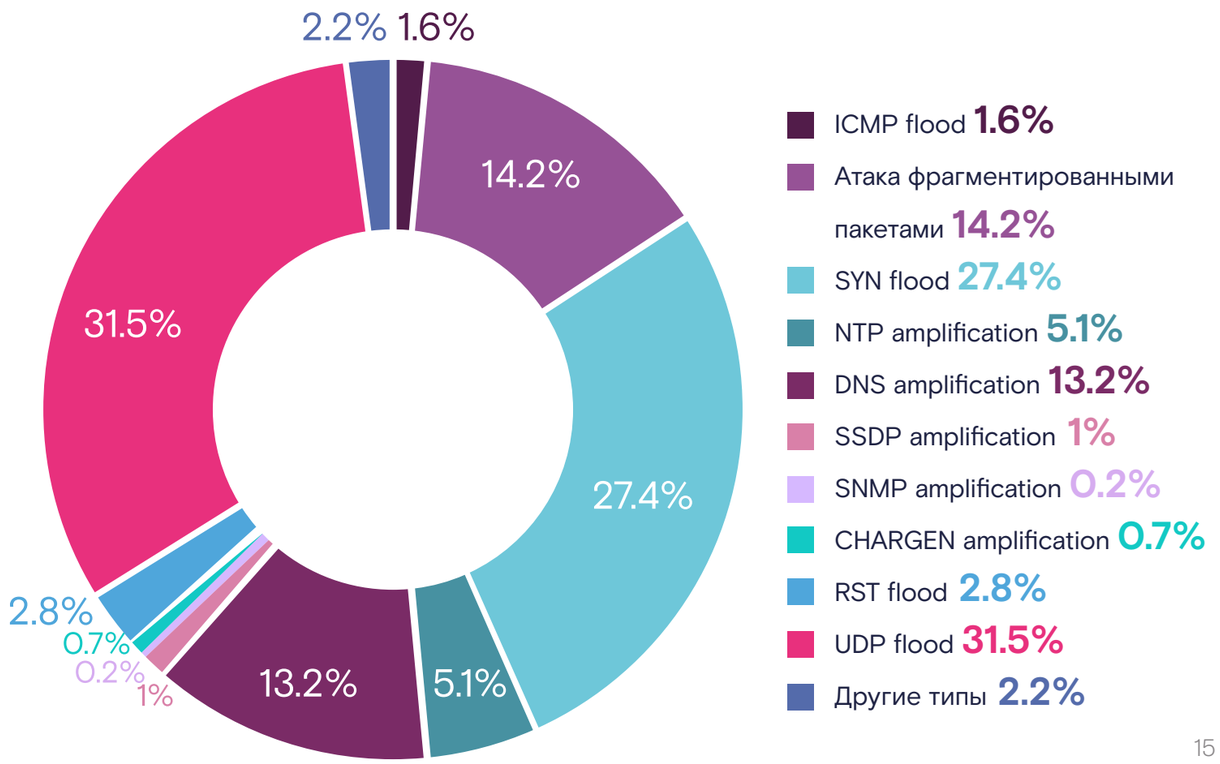
14.2%
атаки фрагментированными пакетами

13.2%
атаки типа DNS amplification

Распределение DDoS-атак по типам, 2018 год



Распределение DDoS-атак по типам, 2019 год



СРАВНЕНИЕ СТАТИСТИКИ С 2017 ПО 2019 ГОДЫ ПОКАЗЫВАЕТ, ЧТО ДОЛЯ АТАК ТИПА UDP FLOOD НЕУКЛОННО СНИЖАЕТСЯ, В ТО ВРЕМЯ КАК ДОЛЯ АТАК ТИПА SYN FLOOD РАСТЕТ ИЗ ГОДА В ГОД. ТО ЕСТЬ АТАКИ НА TCP-СТЕК СТАНОВЯТСЯ ВСЕ БОЛЕЕ ПОПУЛЯРНЫМИ В ПРОТИВОВЕС ОБЪЕМНЫМ АТАКАМ НА КАНАЛ

10.2% → 27.4%

Изменение доли атак типа SYN flood с 2017 по 2019 год

48.8% → 31.5%

Изменение доли атак типа UDP flood с 2017 по 2019 год

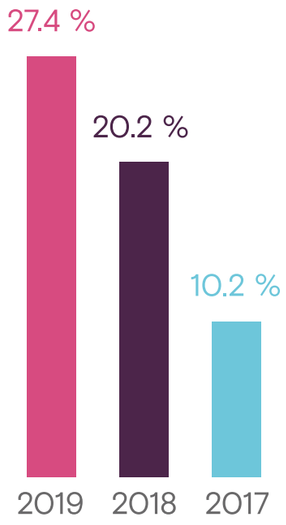
SYN+ACK reflection

Пример комбинированной DDoS-атаки

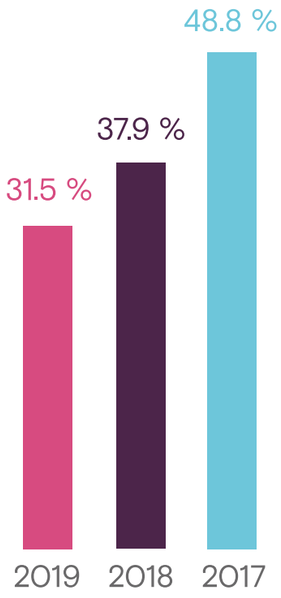
Злоумышленники экспериментируют с редко используемыми сейчас протоколами — 16 (CHAOS) и 111 (IPX over IP). Однако такие атаки скорее исключение: эти протоколы не используются клиентами в реальной жизни и могут быть легко обнаружены и сброшены при подавлении атак.

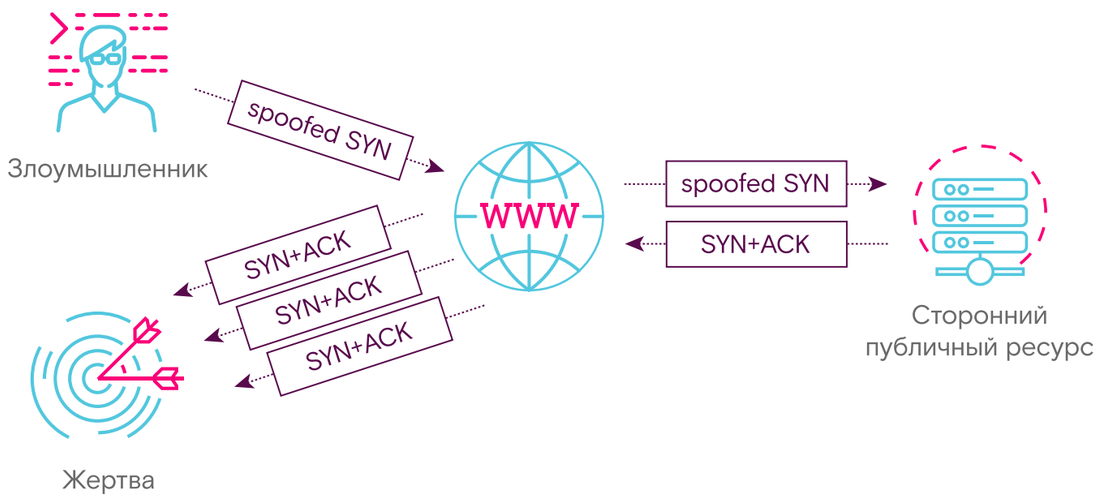
По мере роста уровня защищенности целей злоумышленники начали экспериментировать с видами атак и их сочетанием. Одним из примеров является атака SYN+ACK reflection. Атаки такого типа используют сторонние публичные ресурсы, отправляя на них SYN-пакет с поддельным адресом жертвы в качестве источника. Сторонние серверы отвечают пакетом SYN+ACK жертве, TCP-стек которой страдает от обработки пакетов, пришедших вне всякой сессии. Мы наблюдали ситуацию, в которой обе стороны — и жертва и сторонние ресурсы, используемые для отражения, — были нашими клиентами. У первых это выглядело как SYN+ACK reflection, у вторых как SYN flood.

Распределение атак типа SYN flood



Распределение атак типа UDP flood





Какие прогнозы и как защищаться?

1. Продолжится и расширится использование злоумышленниками устройств Интернета вещей (IoT), так как они позволяют создавать большие ботнеты и усиливать атаки. Проблема усугубится с приходом нового поколения связи 5G и IPv6.

Устраняйте уязвимости во всех ваших устройствах, контролируйте порты, не используйте IPv6. Это усложнит работу злоумышленникам, не дав им использовать соответствующие векторы атак или усилить их.

2. Злоумышленники будут активно использовать существующие векторы атак, их комбинации и амплификаторы, продолжится поиск новых.

Используйте заранее подготовленные варианты противодействия конкретным типам известных атак. Проверяйте свою инфраструктуру. Это поможет правильно настроить защиту в условиях быстро меняющихся векторов атак и не пополнить ряды амплификаторов.

3. Рост количества атак и их мощности продолжится во всех сегментах. Этому будут способствовать ресурсная и экономическая доступность организации DDoS-атак вкупе с их эффективностью.

Как мы помним, основная проблема противодействия DDoS-атакам — это принять и обработать весь поток паразитного трафика, поэтому выбирайте правильные методы защиты. При невозможности купировать атаку, обращайтесь за помощью к сервис-провайдерам или поставщикам услуг.

В целом можно наблюдать, что современные проблемы в области DDoS так или иначе связаны между собой. Это подтверждается атаками 2019 года, когда злоумышленники в рамках одной атаки комбинируют различные типы, меняют векторы, используют амплификаторы и IoT-устройства.

ПОЭТОМУ ЗАЩИТА ДОЛЖНА БЫТЬ КОМПЛЕКСНОЙ: НЕОБХОДИМО ЗАЩИЩАТЬ ИНТЕРНЕТ-ИНФРАСТРУКТУРУ И ВЕБ-ПРИЛОЖЕНИЯ НА РАЗНЫХ ЭТАПАХ ФИЛЬТРАЦИИ

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