2022: годовой отчет StormWall о DDoS-атаках

Отчет StormWall о «DDoS-атаках за 2022 год» — это обзор общей картины атак в 2022 году с разделением на наиболее пострадавшие отрасли и исследование тенденций в области DDoS.

DDoS-атаки эволюционировали в 2022 году

И снова 2022 год стал во многих отношениях рекордным. По мере того, как киберпреступники совершенствовали бот-сети, неуклонно росло количество атак со скоростью несколько терабит в секунду.

Если в 2021 году максимальная мощность атаки составляла около 1 терабита в секунду (Тбит/с), то в этом году она почти удвоилась: в 2022 году атаки, достигающие 2 Тбит/с, стали пугающе частыми.

Аналогичным образом, в течение года неуклонно росла и продолжительность нападений. К концу 2021 года большинству компаний приходилось сталкиваться с инцидентами длительностью до 3 дней.

Всему этому способствовало появление сложных ботнетов. Изначально разработанные хактивистами для политически мотивированных действий, они перешли в руки обычным преступникам.

Начало года ознаменовал резкий всплеск DDoS-активности хакеров и хактивистов в первом квартале. Тенденция перешла во второй квартал, а затем и в третий. И приостановилась в четвертом квартале — активность хактивистов пошла на убыль.

Общие тенденции DDoS-атак в 2022 году

- В целом, количество DDoS-атак в 2022 году увеличилось на 74% по сравнению с аналогичным периодом прошлого года.
- Но в четвертом квартале ситуация изменилась: с конца октября рост атак замедлился и продолжил падение в ноябре. А в декабре количество атак сократилось на целых 53% по сравнению с предыдущим месяцем.
- Год ознаменовался резким увеличением мощности ботнетов, что привело к более сильным и продолжительным атакам.
- Действия киберпреступников были нацелены большей частью на индустрию финтеха. На отрасль пришлось 34% инцидентов. Также в 12 раз увеличилось количество атак на финансовые услуги.

- Хактивисты, разрабатывая инструменты для политически мотивированных действий, сумели увеличить силу и продолжительность атак. А новые сложные ботнеты приняли на вооружение коммерческие преступники.

Статистика DDoS-атак по отраслям

Какие отрасли больше всего пострадали от DDoS:

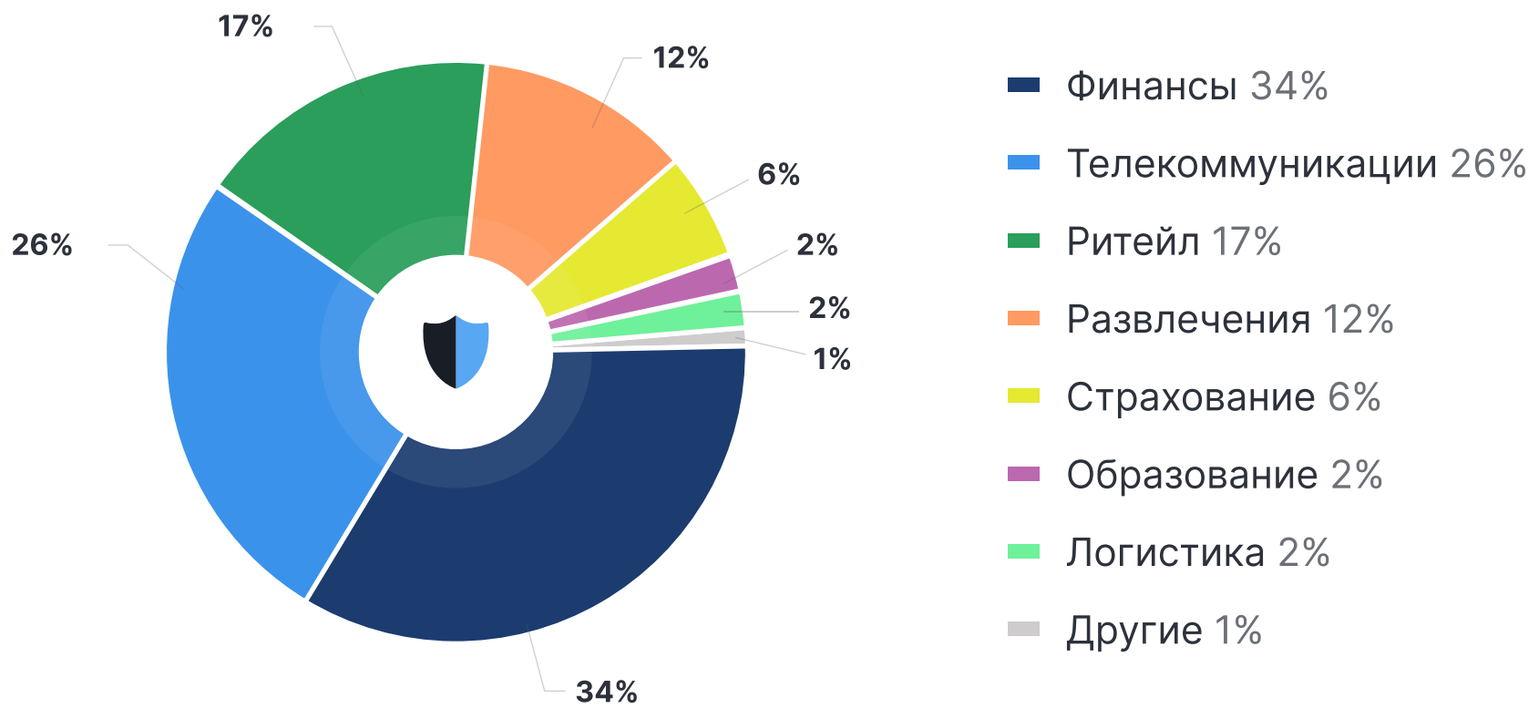

Диаграмма 1. Статистика DDoS атак по отраслям в 2022 году. Источник: StormWall

Финансы

В 2022 году основной удар DDoS-атак пришелся на финансовую индустрию, причем почти треть всех атак (34%) была нацелена на эту сферу.

В этом секторе наблюдался и самый резкий рост атак: их количество увеличилось в 12 раз по сравнению с аналогичным периодом прошлого года.

Индустрия финтеха — традиционно «горячая точка» DDoS-атак: злоумышленники часто проводят мощные атаки на финансовые онлайн-сервисы, чтобы нарушить процесс обработки платежей. Подобное проводится в рамках тактики вымогательства или как дымовая завеса для отведения внимания от одновременного взлома вредоносного ПО или программы-вымогателя. Но в 2022 году множество инцидентов было инициировано хактивистами, особенно в первые два квартала года. Ближе к четвертому кварталу их активность снизилась.

Атаки длились в среднем по 8 часов, а максимальная мощность, наблюдаемая StormWall, достигала 1 миллиона запросов в секунду. Такие атаки возможны только с использованием сложных ботнетов. Это один из примеров, когда инструменты, изначально разработанные хактивистами для собственного использования, начинают получать более широкое распространение, формируя общий ландшафт угроз.

Телекоммуникации

Телекоммуникационная отрасль заняла второе место по количеству атак (26%). Количество атак увеличилось в 4 раза по сравнению с аналогичным периодом прошлого года.

Поскольку пандемия вынудила многие компании перейти на удаленную работу, видеоконференции стали незаменимым элементов критически важных бизнес-процессов. И политически мотивированные злоумышленники, и хакеры осознали эту возможность и начали активно атаковать компании этого сектора. Цели атак варьировались от хактивизма до вымогательства.

Пиковая мощность атаки здесь достигла 1,2 Тбит/с. Средняя продолжительность составила 8 часов. Многие телекоммуникационные компании никогда раньше не сталкивались с киберугрозой такого масштаба. Неподготовленные DDoS-атаки немного нарушили работу их служб, но большинство компаний избежали серьезных сбоев в работе.

Большинство атак на отрасль телекоммуникации можно отнести к попыткам снизить конкуренцию с помощью DDoS. Также кибердары по этой отрасли исходят от хактивистов, постоянно ищущих новые мишени.

Розничная торговля

В 2022 году на отрасль ритейла пришлось 17% DDoS-атак.

При этом количество атак на интернет-магазины увеличилось на 53% по сравнению с аналогичным периодом прошлого года. Большинство инцидентов были вызваны недобросовестной конкуренцией: компании атаковали конкурентов, чтобы привести их магазины к закрытию и увеличить свою долю на рынке.

Как обычно, пик атак пришелся на праздники, когда покупатели устремились в интернет-магазины за подарками и скидками. Резкий скачок атак произошел в феврале за неделю до Дня Святого Валентина (рост на 38% по сравнению с предыдущей неделей) и в ноябре, особенно в преддверии Черной пятницы и киберпонедельника.

Тенденция к более широкому использованию ботнетов здесь сохраняется — некоторые атаки были необычайно мощными, а средняя продолжительность ударов составляла около 3 часов.

Эти данные рисуют тревожную картину. Хотя владельцы онлайн-магазинов давно использовали DDoS-атаки для недобросовестной конкуренции, обычно они прибегали к ботнетам. Эти инструменты требовали определенной технической базы и стоили дорого. Но сейчас все меняется: упрощается процесс запуска ботнетов, дешевле становится поддерживать их длительность. Таким образом, вполне вероятно, что подобные атаки не только продолжатся в 2023 году, но будет расти их сила и продолжительность.

Развлечения

За 2022 год на индустрию развлечений выпало 12% всех DDoS-атак от общего числа атак за год.

Количество инцидентов при этом увеличилось в 3 раза по сравнению с аналогичным периодом прошлого года.

Поскольку карантинные меры во всех странах отменяются, пользователи тратят меньше времени на онлайн-контент. Это несколько уменьшает возможность хакеров использовать время простоя в качестве рычага для вымогательства. Поэтому доля атак на индустрию развлечений снизилась на 12% по сравнению с предыдущим годом, и злоумышленники переключили свое внимание на другие отрасли.

Но общее количество кибератак растет во всех отраслях, что объясняет 5-кратное увеличение общего числа инцидентов.

Страхование

Около 6% DDoS-атак в 2022 году были направлены на предприятия отрасли страхования, что в 5 раз больше по сравнению с аналогичным периодом прошлого года.

Злоумышленники посредством DDoS-атак часто пытаются вымогать деньги у страховых компаний. Конкуренты по бизнесу используют вредоносные программы чтобы занять более прочные позиции на рынке. DDoS-атаки особенно разрушительны для предприятий в этом секторе — они могут привести к значительным финансовым потерям, оттоку клиентов и серьезному репутационному ущербу. В конце концов, для страховщиков имеет первостепенное значение доступность услуг.

Образование

В 2022 году на сферу образования приходилось 2% DDoS-атак. Их количество увеличилось на 36% по сравнению с предыдущим годом.

Зависимость от онлайн-обучения быстро растет после пандемии. Фактически, около 77% студентов государственных колледжей в настоящее время посещают хотя бы один курс онлайн. Но обеспечивающие этот процесс сети недостаточно защищены. А DDoS-атаки сейчас настолько легко запускать, что с этим справятся даже студенты.

Действительно, некоторые из атак, зафиксированные в этом году, были совершены студентами — они атаковали свои академические сети во время экзаменов.

Но многие инциденты были спровоцированы хактивистами, пытавшимися сорвать кампании по приему в вузы России: резкий всплеск атак на университеты страны произошел в первом квартале 2022 года.

Несколько веб-сайтов, которым не хватало профессиональной защиты от DDoS, столкнулись с длительным отключением. Многие критически важные сервисы не работали, из-за чего студенты не могли подать заявления на поступление. Учебным заведениям для восстановления сети поэтому приходилось лихорадочно подключать защиту от DDoS.

Логистика

В 2022 году на долю логистики пришлось 2% DDoS-атак. Наблюдалось увеличение частоты атак на 64% в сравнении с прошлым годом.

Цифровые цепочки поставок предприятий основаны на взаимодействующих компонентах, подобно звеньям в цепи. Многие из них поддерживаются сторонними поставщиками, и клиент в основном должен доверять их способности защитить эти системы. Но некоторые поставщики по-прежнему используют программное обеспечение с открытым исходным кодом, а некоторые из них ослабили меры безопасности в «постпандемическом мире» удаленной работы. Это создает огромную уязвимость и делает устойчивые в других отношениях компании подверженным атакам.

Цепочки поставок настолько прочны, насколько прочно их самое слабое звено, поэтому разрушение одного из звеньев может привести к сбою всей системы поставок. Конечно, хакеры быстро воспользовались этой возможностью, отвлекая команды кибербезопасности DDoS-атаками, устраивали бэкдор-атаки. А это может привести к нарушениям и утечкам конфиденциальных данных.

Но коммерческие преступники были не единственным источником опасности в этом году. Хактивисты также запустили серию крупномасштабных DDoS-атак на логистические предприятия в России в попытке вывести из строя критически важные цепочки поставок.

DDoS-атаки по протоколам

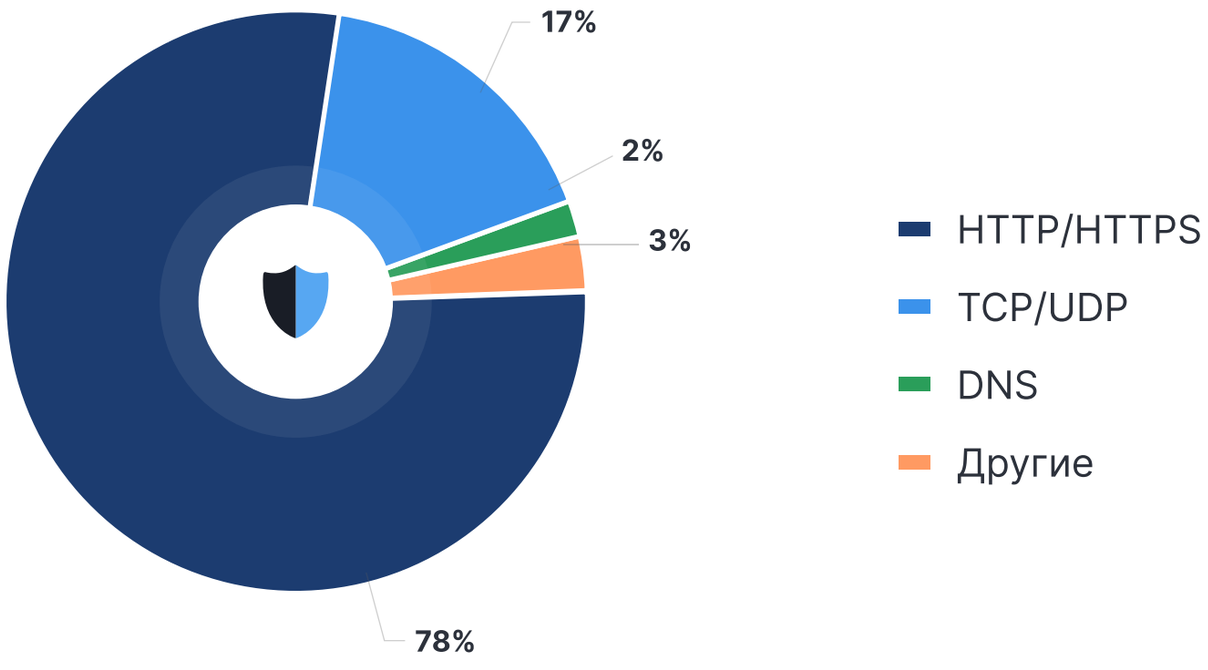

Диаграмма 2. DDoS-атаки по протоколам в 2022 году. Источник: StormWall

Подавляющее большинство DDoS-атак в 2022 году (78%) было направлены на прикладной уровень модели OSI.

Только 17% атак были направлены на сетевой и транспортный уровни, и еще меньше атак на DNS (3%).

Интересно, что по сравнению с прошлым годом распределение атак по протоколам изменилось в обратную сторону. В третьем квартале 2021 года более 80% атак представляли собой лавинную рассылку пакетов, нацеленную на транспортный и прикладной уровни. Поддерживать HTTP-потоки, способные постоянно перегружать корпоративные сети, было просто слишком дорого. В этом году все изменилось, так как стоимость использования сложных ботнетов снизилась, в то время как их огневая мощь, наоборот, многократно возросла.

Это вынудило предприятия переосмыслить защиту от DDoS, поскольку мер безопасности, принятым для повышения их устойчивости к наводнениям TCP/UDP, сегодня недостаточно.

DDoS-атаки по странам

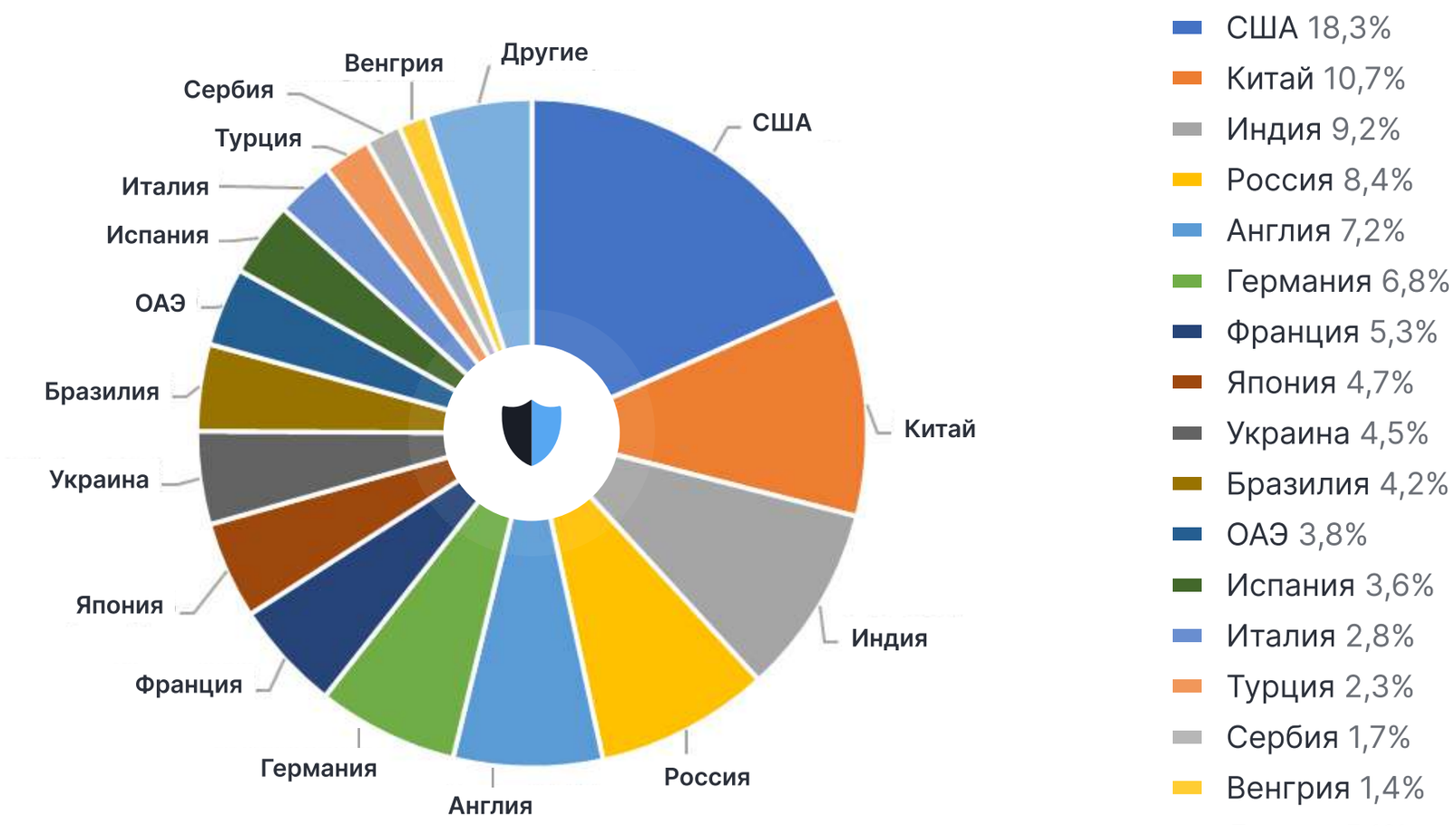

Диаграмма 3. Статистика DDoS-атак по странам. Источник: StormWall

США были атакованы 18,3% от общего числа DDoS-атак, понеся самые тяжелые потери. Как и во всем мире, атаки достигли пика в первом и втором кварталах года. В третьем квартале тенденция изменилась, а в четвертом — снизилась. Злоумышленники были наиболее активны по пятницам, возможно, — в надежде застать службы безопасности врасплох в конце недели.

Китай, на который пришлось 10,7% атак, стал второй по популярности мишенью DDoS-атак прошлого года. Китай — традиционно крупный источник мирового DDoS-трафика.

Индия была близка к тому, чтобы занять нежелательное 2-е место. Но она удостоилась третьего места: на республику было совершено 9,2% от всех инцидентов. Некоторые атаки можно отнести к хактивизму, но это была не единственная причина. Ряд инцидентов были совершен с целью вымогательства или в рамках многовекторных атак.

Россия, четвертая страна по частоте совершенных на неё атак, пострадала от 8,4% общего числа киберугроз в мире.

Очевидно, подобные высокие показатели связаны с российско-украинским конфликтом, который по понятным причинам сделал первую главной мишенью хактивизма. Эксперты StormWall считают, что большая часть нападений исходила от хактивистов — ими двигали политические мотивы. Не имея профессиональных технических знаний, они действовали по инструкции и специализированному ПО инициаторов атаки.

Главный удар DDoS-атак на российские компании был направлен в сектор финтеха (28%), телекоммуникации (18%), госсектор (14%), ритейл (12%), развлекательная сфера (10%), страхование (7%), СМИ (5%), образование (3%), логистика (2%) и остальные (1%).

Таким образом, пострадали все отрасли — от образования до финансов, поскольку независимые и спонсируемые государством банды подвергли страну настоящему обстрелу. Они изо всех сил пытались вывести из строя важнейшую инфраструктуру, парализовать бизнес и банковское дело, а также саботировать экономику в целом.

Более тривиальная история произошла в **Великобритании**, на нее пришлось 7,2% DDoS-атак. Будучи одной из самых развитых экономик в мире, она, как правило, становится мишенью для коммерческих преступников, пытающихся сорвать куш.

Заключение

В этом году киберпреступники значительно продвинулись вперед и практически удвоили свою огневую мощь. К сожалению, то же самое нельзя сказать об устойчивости к DDoS-атакам большинства компаний — продолжительность и мощность атак растет быстрее, чем организации улучшают свои меры по борьбе с ними.

Трудно переоценить последствия этих нападений. В случае успеха они приводят к многодневным простоям, нарушают процесс обучения, ограничивают доступ к информации и даже к банковским операциям. И угроза будет только расти. Вот почему StormWall рекомендует всем компаниям сотрудничать с профессиональным партнером по безопасности, чтобы повысить устойчивость к DDoS-атакам.