

Обзор первого квартала 2023 года: отчет StormWall о DDoS-атаках

StormWall, глобальный провайдер DDoS-защиты, изучил атаки за первый квартал 2023 года на клиентов финансовой отрасли, электронной коммерции, сектора телекоммуникации, развлечений, перевозок, образования и логистики. Результаты представлены в первом отчете StormWall за 2023 год.

Оглядываясь на первый квартал 2023 года

В первом квартале 2023 года общее количество атак уменьшилось по сравнению с аналогичным периодом прошлого года. При этом произошел сдвиг в сторону использования ботнетов и участились DDoS-атаки для прикрытия сложных многоцелевых атак на российские компании — их число выросло на 47% по сравнению с первым кварталом 2022 года.

Злоумышленники также начали смещать акцент на жизненно важную инфраструктуру и услуги, включая логистические службы, центры обработки платежей и банковские системы. При этом они стремятся воздействовать на максимально большее число пользователей.

Фокус на критически важной инфраструктуре, которая обычно хорошо защищена, означал, что киберпреступникам пришлось еще больше увеличить свою огневую мощь.

Зафиксированные нами **атаки достигали максимума в 1,4 Тбит/с и продолжались до четырех дней.**

Одновременный рост продолжительности и пропускной способности был обусловлен растущим применением ботнетов — сетей зараженных устройств. Фактически, **более 38% атак использовали ботнеты в первом квартале 2023 года.**

Обзор тенденций DDoS-атак в первом квартале 2023 года

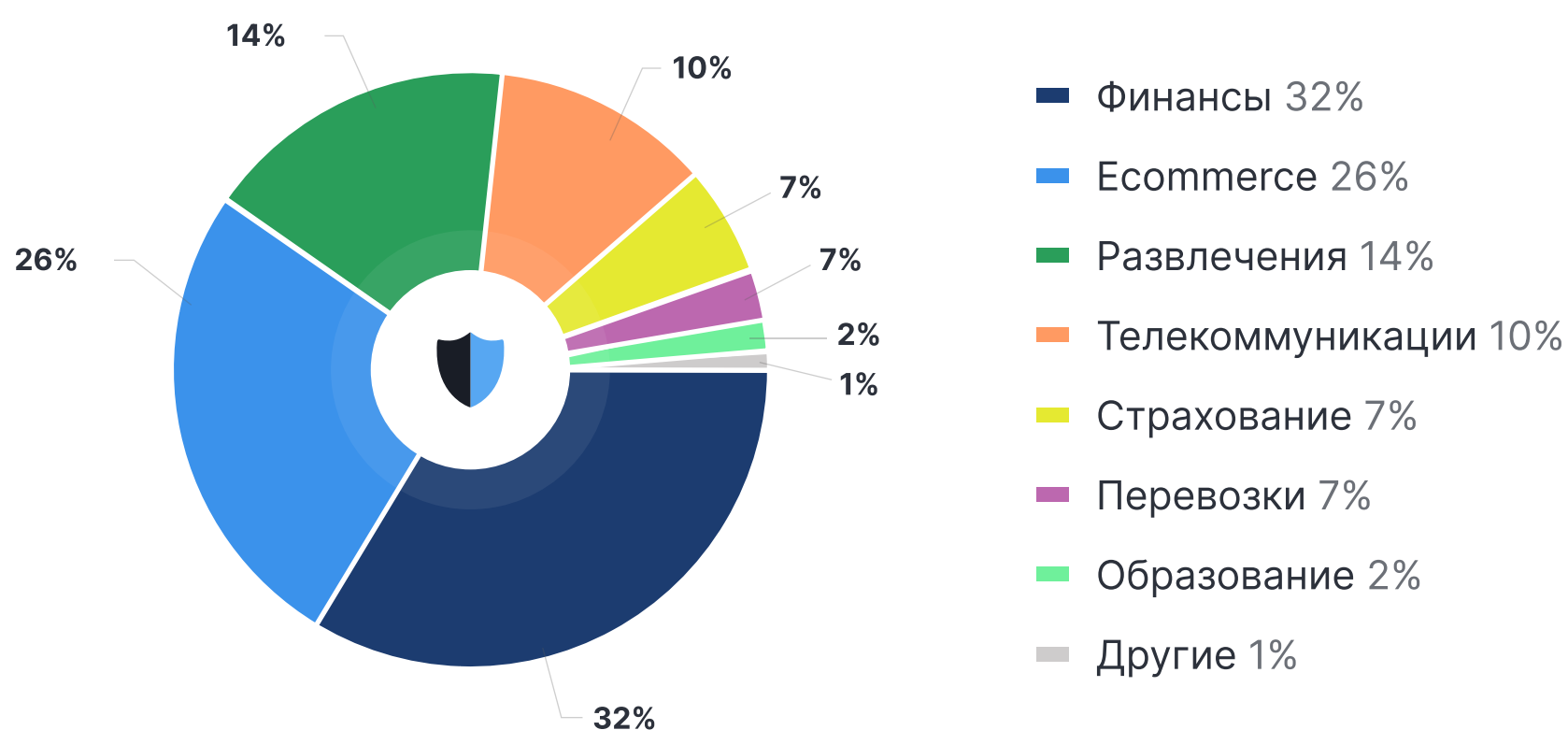
- **Рост отвлекающих маневров:** число DDoS-атак, служивших приманкой в многоцелевых сложных атаках, увеличилось на 47% за год (в сравнении с аналогичным периодом прошлого года). Атаки используются злоумышленниками для отвлечения специалистов по безопасности при проникновении в сети или краже данных.
- **Растущая мощность атаки:** максимальная сила атаки достигла 1,4 Тбит/с, а самая длительная атака шла четыре дня.

- **Нацеленность на критически важную инфраструктуру:** для максимального ущерба киберпреступники сосредоточили свои силы на таких важных сервисах, как платежные системы и центры управления логистикой.
- **Ботнеты продолжают набирать обороты.** Более 38% DDoS-атак использовали сети зараженных устройств.
- **Возобновление числа политических инцидентов:** хактивисты стояли за большинством DDoS-атак на российскую инфраструктуру в 2022 году; в конце 2022 года наблюдалось затишье, но в начале 2023 года возобновились политически мотивированные атаки на российские компании.

Классификация по отраслям: темпы роста DDoS-атак стремительно растут

Частота DDoS-атак резко выросла в большинстве отраслей промышленности, достигнув нового рекордно высокого уровня. Вот распределение инцидентов по секторам за год — начиная от наиболее пострадавших до менее пострадавших сфер

Статистика DDoS-атак по отраслям



1. Финансы

В первом квартале 2023 года главной мишенью был финансовый сектор, на него пришлось 32% атак, количество атак выросло 62% за год.

Атаки на финансовые службы совершались преимущественно для нарушения работы инфраструктуры.

Цели преследовались разные: от вымогательства и шантажа до отвлечения внимания от кражи данных, взлома организаций и продажи конфиденциальной информации в даркнете.

2. Электронная коммерция

Сектор электронной торговли столкнулся со значительными проблемами, — ему пришлось отразить 26% от общего числа атак, что на 38% больше в сравнении с первым кварталом 2022 года.

В первом квартале 2023 года стала разнообразнее направленность атак: под прицел попали не только сайты онлайн-продаж, но и основные сервисы, такие как логистика, цепочки поставок, склады и производители оборудования. Подобное смещение целей контрастирует с прошлыми атаками, когда атаки чаще всего устраивали в праздники конкурирующие компании, чтобы помешать конкурентам и завоевать большую долю рынка.

3. Телекоммуникации

Среди популярных целей для DDoS-атак по-прежнему телекоммуникационная отрасль: на нее было совершено 10% атак, это на 47% больше за аналогичный период прошлого года. Поэтому отрасль занимает третье место по количеству атак.

Все большая цифровизация бизнеса делает жизненно важным бесперебойную доступность телеком-провайдеров. Отключение связи затрагивает многие организации зоны воздействия, предотвращение атак становится для провайдеров огромной нагрузкой. Эта уязвимость делает отрасль главной мишенью для злоумышленников, атакующих ее для вымогательства и шантажа. Также популярна атака на отрасль в качестве отвлекающего маневра, посредством которого хакеры стремятся похитить конфиденциальные данные у поставщиков услуг связи.

4. Развлечения

Индустрия развлечений отразила значительное количество DDoS-ударов — 14% за первый квартал 2023 года, что на 97% выше аналогичного периода за 2022 год.

Больше всего пострадали стриминговые платформы и серверы онлайн-игр. Труднее пришлось компаниям без профессиональной защиты от DDoS: длительные сбои в работе лишили многих игроков возможности наслаждаться своими любимыми играми.

Пользователи переходили к конкурентам с более защищенной инфраструктурой, выдержавшей атаки. Соответственно, компании без DDoS-защиты потерпели финансовые и репутационные потери, снизилась их рыночная доля.

5. Перевозки

Транспортная отрасль ощутила самый резкий рост числа DDoS-атак. Несмотря на то, что на долю этого сектора пришлось всего 7% объема атак, количество атак выросло на 118% в сравнении с аналогичным периодом прошлого года.

Транспортные узлы, такие как центры управления дорожным движением, аэропорты и транспортные компании, были главными целями злоумышленников. Эта тенденция вызывает беспокойство. Как и большинство сервисов, центры управления транспортом полагаются на подключение к Интернету для бесперебойной работы таких систем, как светофоры, сигнализация в метро и средства автоматизации поездов.

Неисправные системы могут вызвать значительные задержки в работе транспортных узлов, а это приводит к миллионным убыткам и создает непосредственную угрозу для общественной безопасности. Приоритетность защиты транспортных систем от DDoS-атак имеет решающее значение, особенно с учетом того, что мы ожидаем дальнейшего роста числа атак на этот сектор.

Страхование и образование

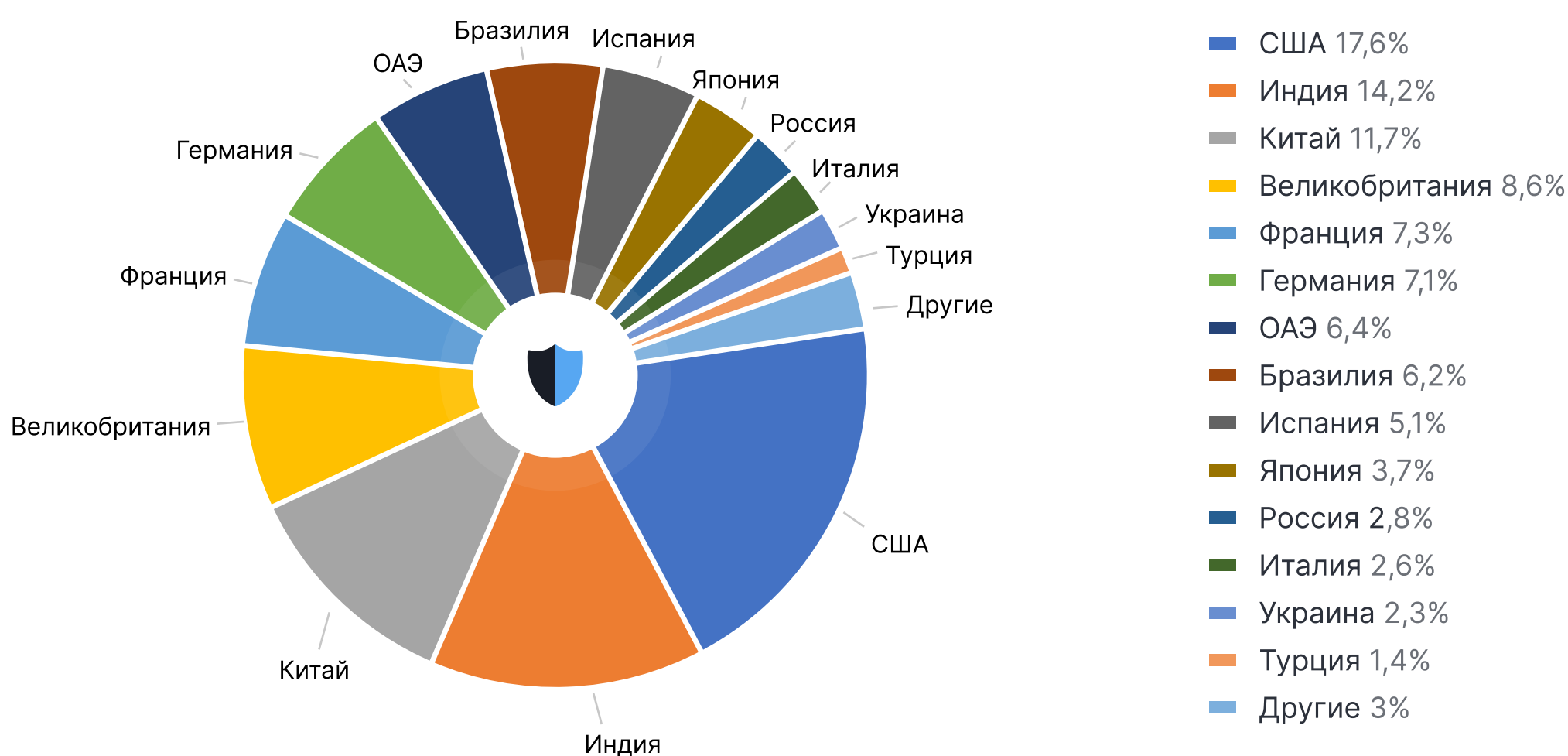
Темпы роста DDoS-атак в сфере страхования и образования стабилизировались: доля атак составила 7% и 2%, соответственно. Инциденты в сфере образования выросли на 16%, в сфере страхования — на 5%.

Прошлогодний всплеск атак на сектор онлайн-обучения, отчасти вызванный хактивизмом, пошел на убыль в 2023 году. По мере снятия ограничений и возвращения учащихся в школы количество атак со стороны учащихся, пытающихся уклониться от экзаменов, также сократилось. В страховом секторе хакеры в первую очередь искали возможности для вымогательства и шантажа.

Классификация DDoS-атак по странам

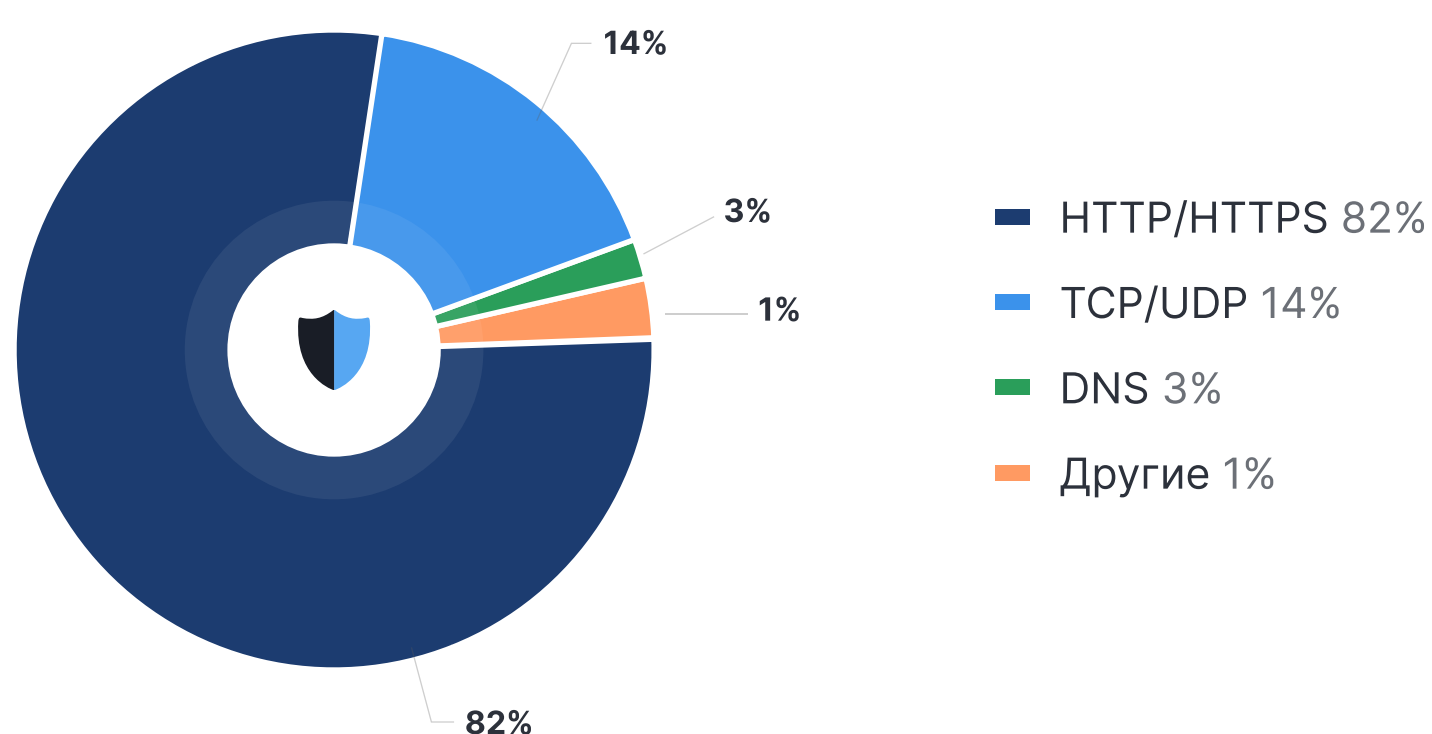
США, Китай и Индия продолжают возглавлять список наиболее DDoS-атакуемых стран. Заметный всплеск атак наблюдался в Объединенных Арабских Эмиратах: доля атак выросла почти вдвое — с 3,8% в первом квартале 2022 года до 6,4% в текущем году. И наоборот, как в России, так и на Украине наблюдалось снижение активности DDoS-атак, что привело к снижению рейтинга.

Ниже приведена статистика DDoS-атак по странам:



DDoS-атаки по протоколам

В первом квартале 2023 года продолжают набирать обороты ботнеты, в результате количество атак на уровне приложений растет. С другой стороны, количество атак на транспортном уровне, таких как SYN-флуд или UDP-флуд, сокращается.



Флуд-атаки на более низкие уровни модели OSI обычно менее разрушительны, чем атаки прикладного уровня. Хотя первые и могут привести к перегрузке и потере пакетов, ресурс не перестает полностью отвечать на запросы. А это значит, что чем доступнее и экономически эффективнее становятся более разрушительные атаки на прикладном уровне, тем меньше причин совершать TCP/UDP флуд, только он не нацелен на службу, специально уязвимую для этого типа атак.

Вывод

В первом квартале 2023 года наблюдался почти повсеместный рост объема, силы и продолжительности атак. При этом появляются новые тенденции к смещению внимания на транспортные узлы, что подчеркивает растущую угрозу DDoS-атак.

Вызывает беспокойство то, что злоумышленники адаптировали свою тактику, интегрируя DDoS-атаки в многовекторные инциденты. По этой причине организациям пришлось решать проблемы не только с перебоями в работе из-за перегрузки серверов, но и с утечками данных, программами-вымогателями и другими угрозами. Подобные тенденции характерны уже для первого квартала 2023 года — это настораживает и заставляет задуматься об их возможной эскалации в будущем.

На основе анализа данных атак, StormWall прогнозирует рост DDoS-атак на 170% к концу 2023 года. Рекомендуем всем предприятиям обратиться за профессиональной защитой от DDoS-атак, чтобы обеспечить свою безопасность в предстоящем году.