Отчет об атаках на онлайн-ресурсы российских компаний в I полугодии 2024 года

Введение

Первая половина 2024 года показала, что онлайн-ресурсы по-прежнему остаются одной из ключевых целей хакеров. Продолжительность DDoS-атак заметно снизилось. Однако киберпреступники значительно нарастили количество атак и стали использовать более изощренные методы для их проведения, такие как мультивекторный DDoS.

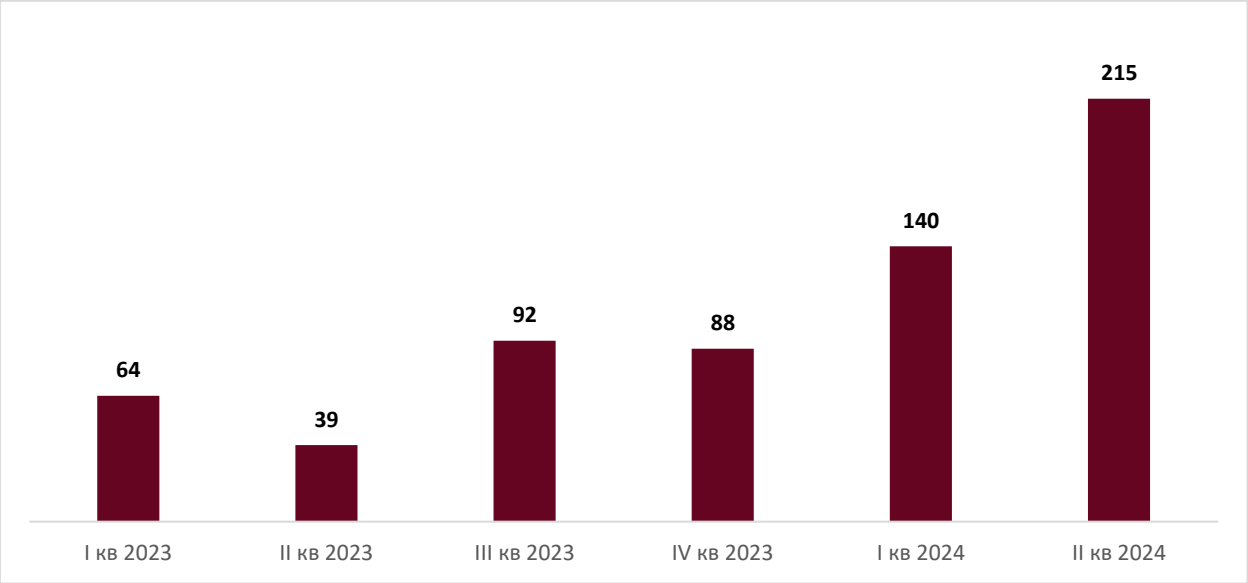
Данный отчет отражает картину того, как киберпреступники использовали DDoS- в I полугодии 2024 года. Аналитика составлена на основе данных об атаках, зафиксированных и отраженных сервисом Anti-DDoS ГК «Солар» с января по июнь 2024 года в сравнении с аналогичным периодом 2023 года. Учтена информация о массовых атаках на магистральные каналы связи, сетевую инфраструктуру доступа к услугам и клиентское оборудование.

Для отчета была проанализирована информация почти о 700 компаниях из различных отраслей, включая ретейл, финансы, госсектор, грузопассажирские перевозки, телекоммуникации и другие, находящиеся под защитой сервиса Anti-DDoS ГК «Солар».

Какими были DDoS-атаки в I полугодии

В первом полугодии 2024 года эксперты ГК «Солар» зафиксировали 355 тыс. DDoS-атак на российские организации – это на 16% больше, чем за весь 2023 год. Этот резкий рост показывает, что без надлежащей защиты от DDoS организации остаются в неведении, пытаясь справиться с атаками, которые приносят бизнесу серьезные убытки.

Статистика по количеству DDoS-атак, тыс. штук



Частота ежедневных атак в I половине 2024 года выросла более чем в 4 раза в сравнении с аналогичным периодом 2023 года. Угрозы в первую очередь направлены на создание цифрового хаоса, чтобы нарушить важные цепочки продаж и лишить дохода российские компании и организации, а также затруднить жизнь россиян.

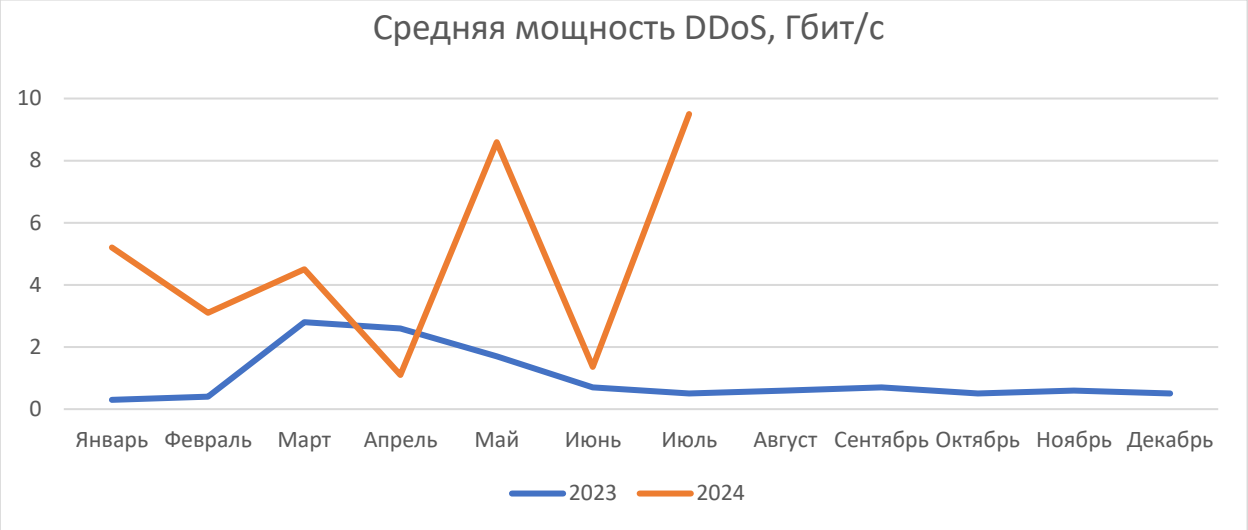
Рост обусловлен несколькими ключевыми факторами. Во-первых, аренда вычислительных мощностей делает создание ботнетов доступнее, что позволяет злоумышленникам с легкостью обрушивать огромное количество трафика на целевые системы. Во-вторых, легкость заражения и распространения вирусов среди различных цифровых устройств способствует увеличению числа участвующих в атаках девайсов. Кроме того, «порог вхождения» в DDoS-атаки стал ниже благодаря наличию бесплатных, дешевых и доступных инструментов, что привлекает все большее количество злоумышленников.

Мощность атак

В первом полугодии 2023 года максимальная зафиксированная мощность DDoS-атаки составила 174 Гбит/с. Это уже само по себе значительное значение, способное вызвать существенные перебои в работе целевых систем – особенно, если они не оснащены достаточной защитой.

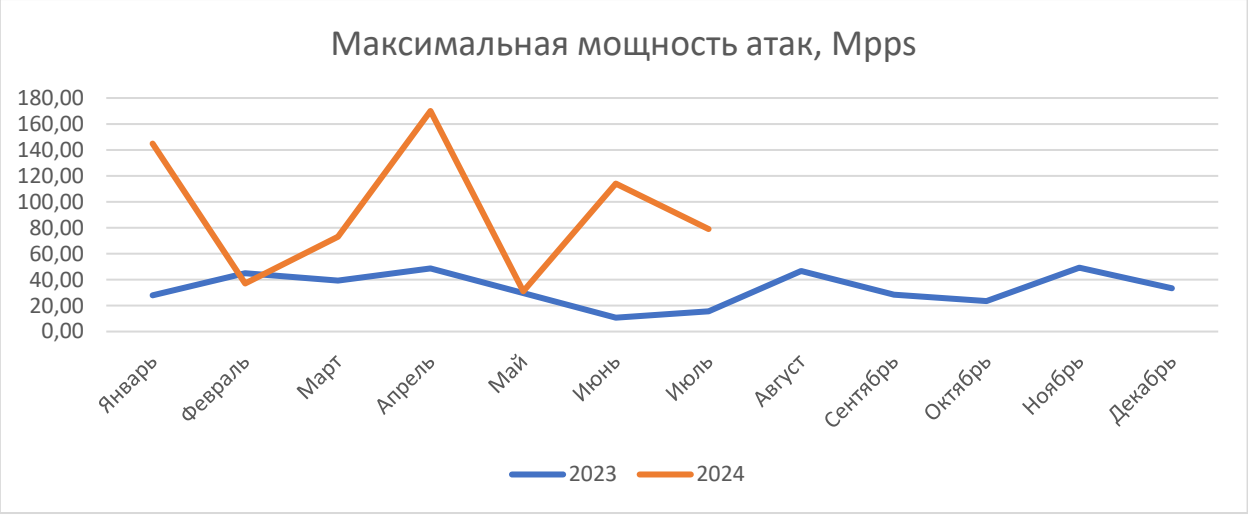
Однако в первом полугодии 2024 года мы наблюдаем радикальное усиление: мощность самой крупной зафиксированной атаки достигла 1,2 Тбит/с. Увеличение в 6,7 раза по сравнению с аналогичным периодом прошлого года указывает на развитие угроз. Это означает, что сегодня хакеры оснащены более мощными ботнетами и используют еще более сложные техники нападения. Также рост подчеркивает острую необходимость адаптации и усовершенствования мер защиты – как с технологической точки зрения, так и в части выстраивания ИБ-стратегии и подготовки специалистов по кибербезопасности.

В свою очередь, средняя мощность атак за первое полугодие 2023 года составила 2,4 Гбит/с, в то время как в аналогичном периоде 2024 года она увеличилась до 4 Гбит/с. Это может указывать на изменение тактик атакующих, которые, вполне вероятно, сосредоточились на более изощренных методах.



Интенсивность DDoS-атак также можно оценивать в количестве пакетов в секунду (PPS).

В первом полугодии 2024 года максимальная интенсивность атаки выросла до 170 Mpps – более чем в три раза в сравнении с аналогичным периодом 2023 года. Это значит, что уже сегодня хакеры нарастили мощности и готовы проводить более масштабные и интенсивные атаки.

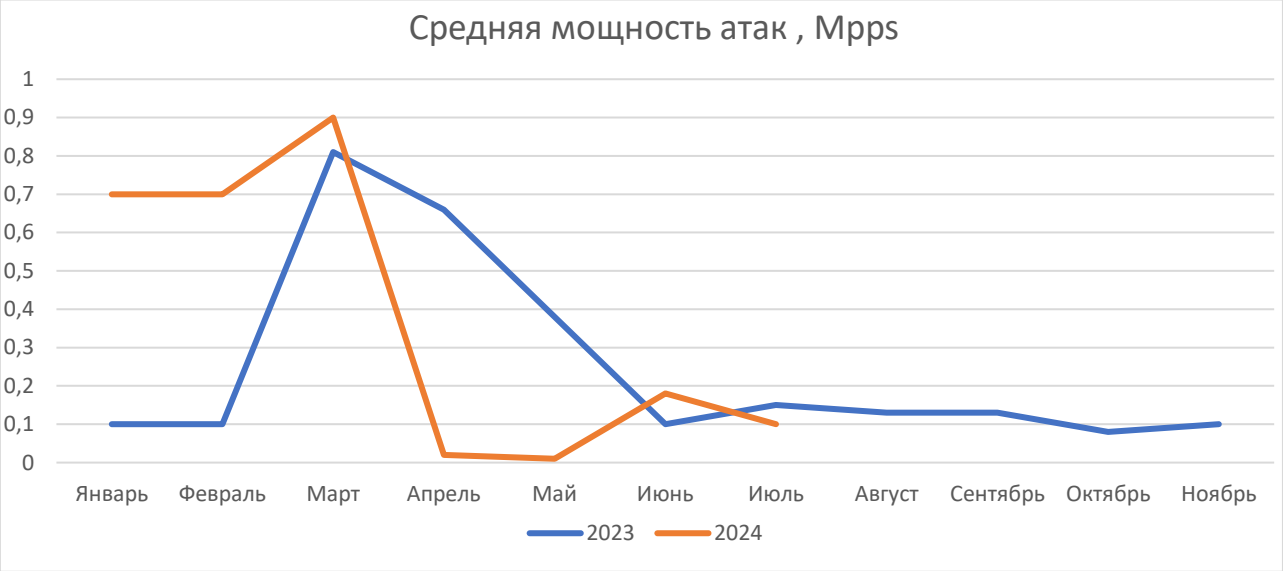


При этом одним из трендов 2024 года является создание ботнетов не из зараженных устройств, а за счет аренды вычислительных мощностей в облачных ЦОДах по всему миру с автоматизированной монетизацией и сдачей в аренду под инструменты DDoS-атак.

Средняя интенсивность атаки в Mpps в I полугодии 2024 года осталась без изменений в сравнении с аналогичным периодом 2023 года – до 0.4 Mpps (418,8 PPS). Это может свидетельствовать о развитии различных типов атак,

направленных на исчерпание ресурсов целевых систем в течение более продолжительного времени.

Однако проведение дистанционного электронного голосования в марте ознаменовалось значительным всплеском средней мощности, что свидетельствует о возросшей уязвимости критически важных цифровых систем в условиях повышенной активности хакеров, которые стремились вызвать дестабилизацию серверов наиболее критичных российских организаций и тем самым подорвать доверие граждан к процессу голосования.



Продолжительность

В I полугодии 2023 года максимальная продолжительность DDoS-атаки составила 109 дней, а средняя – 195 минут, что равно 3 часам 15 минутам. При этом самый продолжительный DDoS в прошлом году в совокупности длился 9 месяцев. В I

полугодии 2024 года максимальная продолжительность DDoS-атаки снизилась более чем в три раза, до 35 дней, а средняя уменьшилась в 24 раза – до 8 минут.

Основной причиной резкого снижения продолжительности DDoS-атак можно назвать изменение тактики злоумышленников. Хакеры стали выбирать более краткосрочные и целевые атаки, чтобы избежать обнаружения и более эффективно использовать свои ресурсы. Такие атаки в первую очередь направлены на быстрый и внезапный сбой систем за счет повышения их количества и интенсивности, а не на долгосрочное истощение ресурсов жертвы. Эта тактика может сбивать с толку защитные системы, которые настроены на определение более продолжительных атак.

Однако повышение эффективности средств защиты может вызвать дальнейшие изменения в тактике хакеров, которые могут сосредоточиться на еще более краткосрочных, но высокоэффективных атаках, наносящих максимальный ущерб за очень короткое время. В связи с этим эксперты ГК «Солар» рекомендуют российским организациям переводить критичные системы на постоянную тонкую фильтрацию DDoS-атак, чтобы сократить время определения и отражения атаки.

Векторы DDoS-атак

В I полугодии 2024 года мы выявили значительные изменения в распределении и характере векторов DDoS-атак. На основе собранных данных можно наблюдать тенденции роста некоторых типов атак, а также особенности мультивекторных DDoS-атак, которые представляют наибольшую угрозу для безопасности сетевой инфраструктуры.

Топ-5 типов DDoS-атак в первой половине 2024 года:

1. MultiVector

Мультивекторные DDoS-атаки включают в себя несколько типов атак одновременно. Это могут быть комбинации SYN Flood, UDP Flood, ICMP и других векторов. Сегодня это наиболее значительная угроза для сетевой инфраструктуры, поскольку злоумышленники все чаще используют комбинированные методы для увеличения разрушительной силы атаки.

2. SYN Flood

SYN Flood направлен на создание большого числа неполных соединений, что приводит к исчерпанию ресурсов сервера и его недоступности для легитимных пользователей. В прошлом году 90% мощных кибератак приходилось на SYN Flood, и сегодня число атак такого типа в первом полугодии 2024 года выросло в 4,5 раза год к году, до 60 тысяч. Это свидетельствует о повышенной активности злоумышленников, нацеленных на перегрузку серверных ресурсов.

3. UDP Flood

Атаки типа UDP Flood создают огромный объем UDP-трафика, направленного на исчерпание пропускной способности сети и перегрузку целевых серверов. UDP Flood остается популярным методом атак, особенно в контексте мультивекторных атак.

4. SUNRPC

Атаки такого типа сохранили свою значимость и в 2024 году, что указывает на продолжающуюся уязвимость систем, использующих данный протокол.

5. ICMP

ICMP, также известные как Ping Flood, создают огромный объем ICMP Echo-запросов, что может привести к перегрузке целевых серверов. Такие атаки стали более распространенными в 2024 году в составе мультивекторных атак.

Тенденции и проблемы мультивекторных DDoS-атак

Мультивекторные DDoS-атаки представляют собой одну из самых серьезных угроз для современных сетевых инфраструктур. В 2024 году эти атаки стали особенно заметны благодаря своей способности обходить традиционные механизмы защиты и создавать масштабные перебои в работе систем. Основные проблемы мультивекторных атак включают:

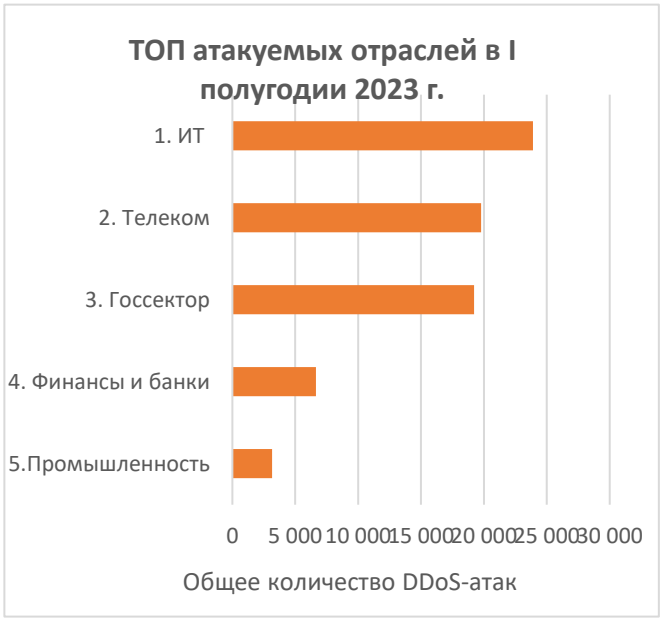
1. **Сложность в обнаружении.** Мультивекторные атаки используют сразу несколько методов одновременно. Например, DDoS-атака может начинаться как SYN Flood, а затем переходить на UDP Flood или ICMP. Подобные методы усложняют обнаружение и защиту от атак.
2. **Повышенная разрушительная сила.** Использование нескольких векторов одновременно значительно увеличивает нагрузку на системы, что может привести к их быстрому выходу из строя. Особенно это касается атак на критически важные инфраструктуры, такие как DNS или службы аутентификации.
3. **Необходимость комплексного подхода к защите.** Для защиты от мультивекторных атак требуется внедрение комплексных систем защиты, которые способны быстро адаптироваться и реагировать на изменения вектора DDoS-атаки.

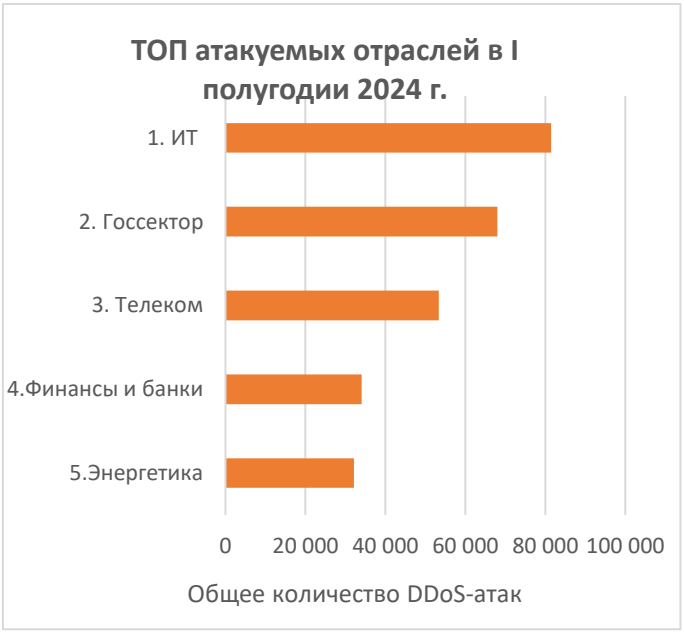
Также в I полугодии 2024 года наблюдается значительное увеличение числа атак на DNS – их количество в первой половине текущего года выросло более чем в 2 раза в сравнении с аналогичным периодом 2024 года – до 22 тыс. атак. Это свидетельствует о повышенном интересе злоумышленников к компрометации и перегрузке DNS-серверов, что может привести к значительным перебоям в работе интернет-сервисов российских организаций и госструктур.

Для эффективной защиты от подобных угроз эксперты ГК «Солар» рекомендуют внедрять продвинутые систем анализа трафика и использовать гибкие стратегий защиты от DDoS-атак, способных адаптироваться к меняющимся условиям киберпространства.

Кого атаковали

DDoS-атаки остаются одной из ключевых угроз для различных отраслей, особенно в контексте роста прямых атак и изменения методов использования инфраструктуры для запуска атак. Например, в 2024 году мы наблюдаем увеличение активности злоумышленников, арендующих мощности на отечественных облачных платформах и используя для атак искусственные ботнеты внутри страны. Это, в свою очередь, вызывает проблемы при их обнаружении и фильтрации.





Как мы видим, ИТ-сектор остался лидером по количеству DDoS-атак. Компании из данной отрасли часто становятся целью хакеров из-за критической значимости для совершения многих бизнес-процессов огромного количества российских организаций, а также из-за объемов обрабатываемых данных.

Также более чем в 3,5 раза год к году выросло число DDoS-атак на госсектор. Это лишь подтверждает нашу теорию о том, что сегодня настроены на максимальный деструктив и стремятся нарушить работу государственных функций, многие из которых прямым образом влияют на жизнь российских граждан.

Увеличение атак в телекоммуникациях более чем в 2,5 раза в сравнении с аналогичным периодом 2023 года связано с попытками злоумышленников нарушить доступ к критическим услугам связи.

Также в I полугодии 2024 года в 5 раз в сравнении с тем же периодом прошлого года выросло число атак на кредитно-финансовую отрасль. Хакеры стараются привести к неработоспособности сразу множество банков за счет большого количества коротких кибератак, чтобы оказать негативное влияние на россиян.

Помимо этого, в ТОП-5 наиболее атакуемых российских отраслей попала отрасль энергетики – количество DDOS-атак на данный сектор за год выросло в 19 раз. Это свидетельствует о том, что злоумышленники все чаще нацеливаются на критическую инфраструктуру, которая имеет прямое влияние на экономику и безопасность. Также тренд подчеркивает необходимость укрепления защиты в энергетической отрасли.

Мы прогнозируем, что в 2024 году продолжится тренд на рост DDoS-атак на критическую инфраструктуру и финансовый сектор, вероятно, что требует адаптации защитных мер.

География атак

Москва остается наиболее атакуемым регионом РФ, что связано с высокой концентрацией важных государственных и финансовых структур в столице.

Отдельно отметим, что количество атак в Поволжье выросло в 6 раз. Регион вызывает все больше интереса у хакеров – возможно, это связано с ростом экономической активности и развитием инфраструктуры в регионе. Также почти в 5 раз выросло число DDoS-атак на Юге, что может говорить о повышении интереса проукраински настроенных хакеров к региону в связи с развитием геополитических событий.

Выводы по DDoS-атакам в I полугодии

Злоумышленники демонстрируют высокую степень адаптации и изменения используемой инфраструктуры для DDoS-атак. Первая половина 2024 года показала, что DDoS-атаки становятся все более серьезной угрозой для российских компаний, особенно для государственных структур и отраслей, прямо влияющих на российскую экономику и безопасность населения.

Хакеры переключились на массовые кратковременные DDoS-атаки невысокой мощности, а также стали применять мультивекторные атаки, которые способны нарушить работу онлайн-сервисов, если не применять продвинутые методы защиты.

В этом контексте ГК «Солар» играет ключевую роль, предлагая сервис Anti-DDoS для фильтрации трафика, способный отражать в том числе мультивекторные атаки любой мощности.