SOLAR

ОТЧЕТ

ОТЧЕТ ОБ АТАКАХ НА ОНЛАЙН-РЕСУРСЫ РОССИЙСКИХ КОМПАНИЙ В 2023 ГОДУ

W: RT-SOLAR.RU

МОСКВА 2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В 2023 году сохранился ландшафт угроз для онлайн-ресурсов, которые по-прежнему остаются одной из ключевых целей киберпреступников. Несмотря на то что количество DDoS- и веб-атак за год сократилось, их интенсивность и максимальная мощность растет.

Данный отчет отражает картину того, как киберпреступники использовали DDoS- и веб-атаки в минувшем году. Аналитика составлена на основе данных об атаках, зафиксированных и отраженных сервисами Anti-DDoS и WAF платформы Solar MSS ГК «Солар» с января по декабрь 2023 года. Учтена информация о массовых атаках на магистраль, канальную инфраструктуру доступа к услугам, клиентское оборудование, а также о веб-атаках на опубликованные в интернете онлайн-приложения организаций.

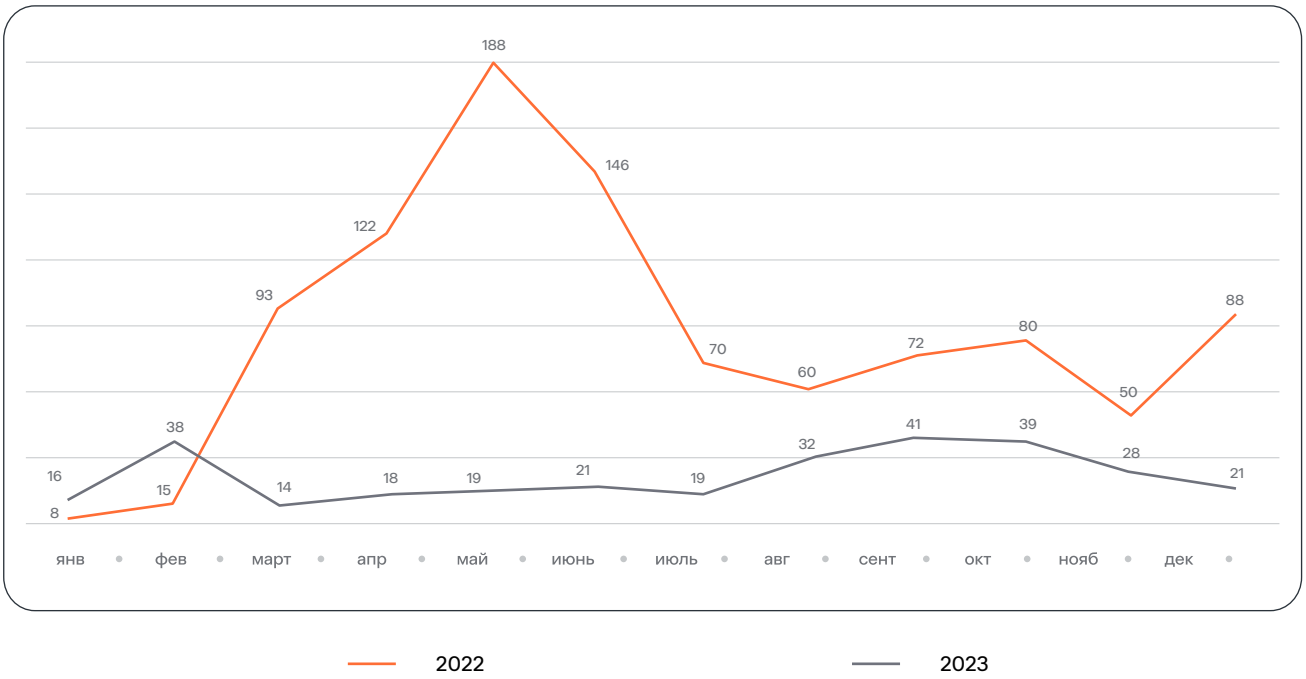
Для отчета была проанализирована информация почти о 700 компаниях из различных отраслей, включая ретейл, финансы, госсектор, грузопассажирские перевозки, телекоммуникации и другие.

КАКИМИ БЫЛИ DDOS-АТАКИ В 2023 ГОДУ

В данной главе описаны атаки, зафиксированные и отраженные сервисом мониторинга трафика и защиты от DDoS-атак (Anti-DDoS). DDoS-атака – это действия злоумышленников, направленные на нарушение работоспособности инфраструктуры организации, ее порталов и веб-ресурсов.

Хакеры искусственно создают нелегитимный трафик, чтобы сделать сайты недоступными для пользователей.

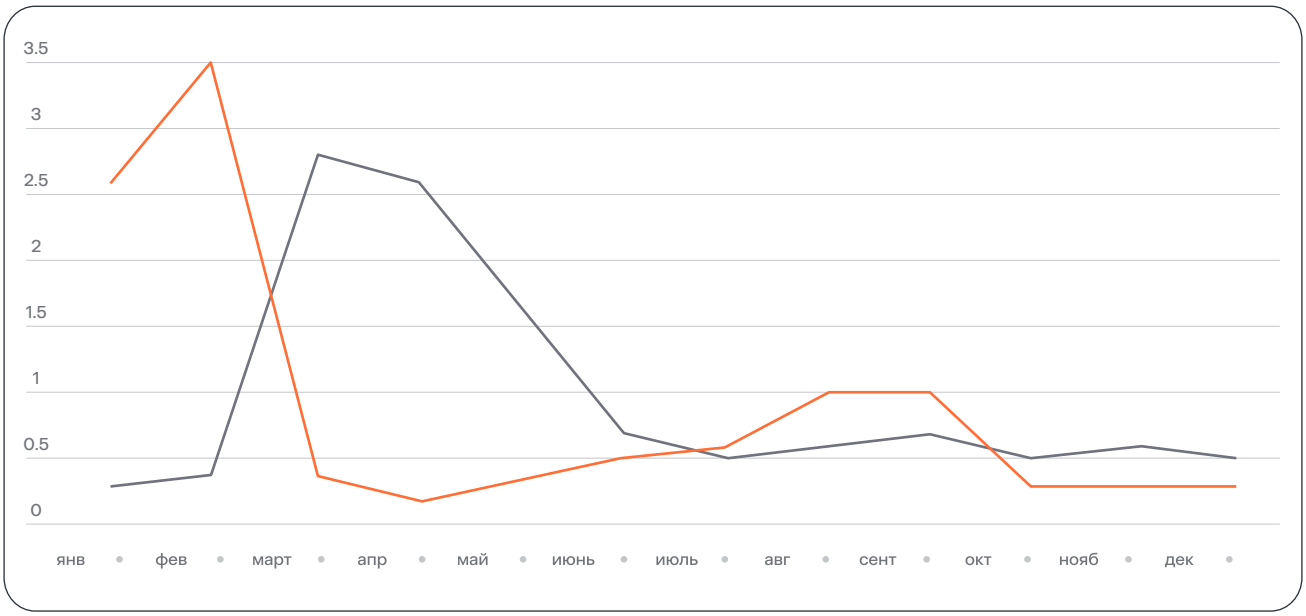
Количество DDoS-атак по месяцам, тыс. штук



В 2023 году эксперты ГК «Солар» зафиксировали 306 тыс. DDoS-атак на российские организации, что почти в три раза меньше аналогичного показателя 2022 года. При этом если в первом полугодии 2023 года атак было в 4 раза меньше, чем годом ранее, то с августа разрыв стал сокращаться. В итоге во втором полугодии 2023 года было зафиксировано в два раза меньше атак, чем за аналогичный период предыдущего года.

Такая разница в показателях может быть связана с возросшей активностью злоумышленников сразу после начала СВО, когда большинство российских компаний столкнулись с волной атак на свои онлайн-ресурсы. Отчет за 2022 год можно найти по ссылке. Позже DDoS отыграл аномальный рост и вернулся к более стандартным значениям. Не исключено, что на фоне линейного роста DDoS, уже к осени текущего года атаки достигнут показателей 2022 года.

Средняя мощность DDoS, Гбит/с



Средняя мощность DDoS в 2023 году оказалась чуть ниже, чем в 2022-м. В большинстве месяцев, как в 2022, так и в 2023 году, средняя мощность атак не превышала 1 Гбит/с.

Если учесть, что большая часть коммерческих компаний использует каналы шириной до 100 Мбит/с (0,1 Гбит/с), то средняя мощность DDoS может быть критичной для многих организаций.

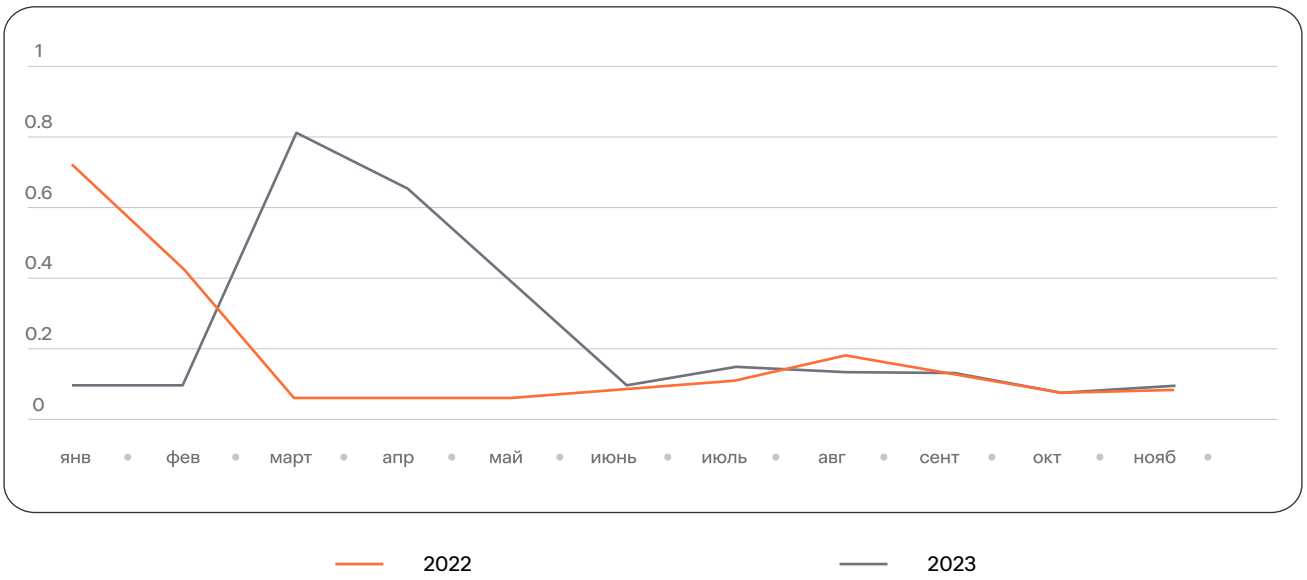
Максимальная мощность атак, Гбит/с

В четвертом квартале 2022 года максимальная мощность атак существенно снизилась – до 2 Гбит/с. С такого же значения начался и 2023 год. Но с марта показатель начал расти, и к концу года, когда динамика максимальной мощности DDoS вернулась к уровню 2022 года (до 500 Гбит/с), превысил самую мощную атаку 2022 года (768 Гбит/с). Это говорит о попытках злоумышленников нарастить свои возможности для реализации прицельных мощных кибердударов. В частности, можно ждать мощного DDoS на онлайн-ресурсы, связанные с президентскими выборами в России в марте 2024 года. Также не исключено, что таким образом хакеры тестируют ПО для управления крупными ботнетами, способными реализовывать масштабный DDoS.

1 ТБИТ/С

составила самая мощная DDoS-атака в 2023 году

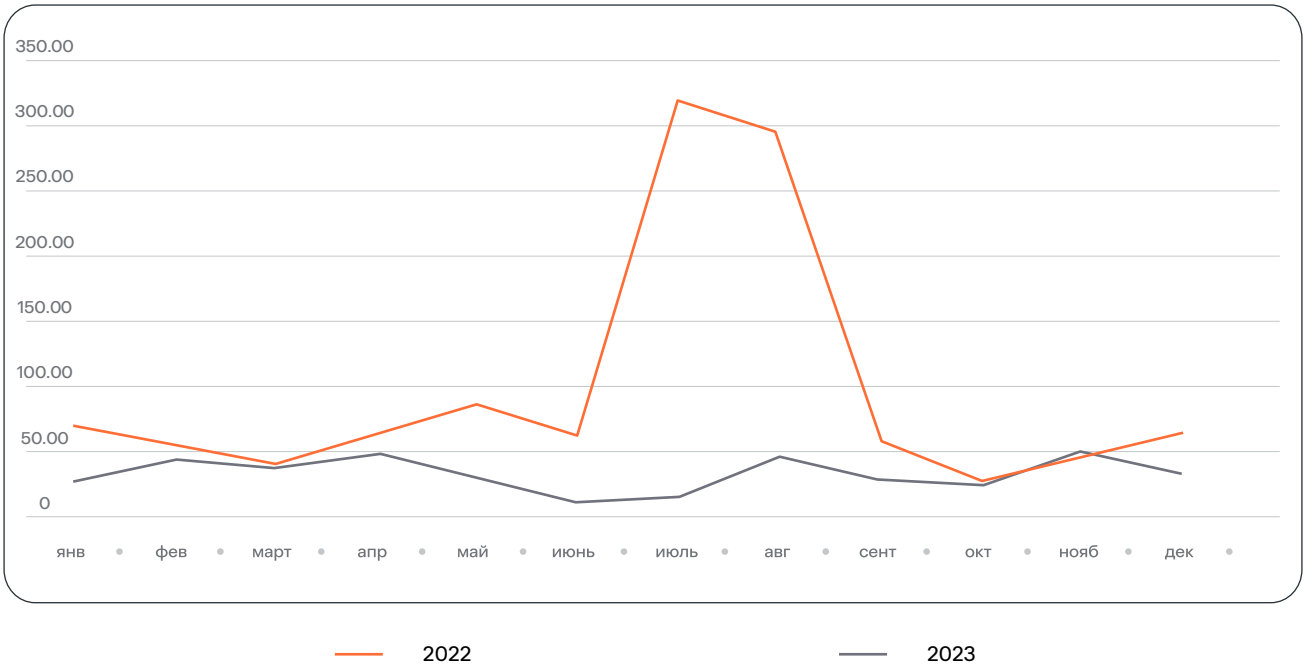
Средняя мощность атак , Mpps



По средней мощности в миллионах пакетов в секунду (Mpps) первое полугодие 2023 года обгоняет аналогичный показатель предыдущего года. Вторая половина 2023 года по динамике и величинам Mpps совпадает с 2022 годом.

DDoS-атаки по максимальной мощности в Mpps показали равномерную динамику в течение 2023 года на уровне примерно 40 Mpps, что совпадает с динамикой по большинству месяцев 2022 года.

Максимальная мощность атак, Mpps

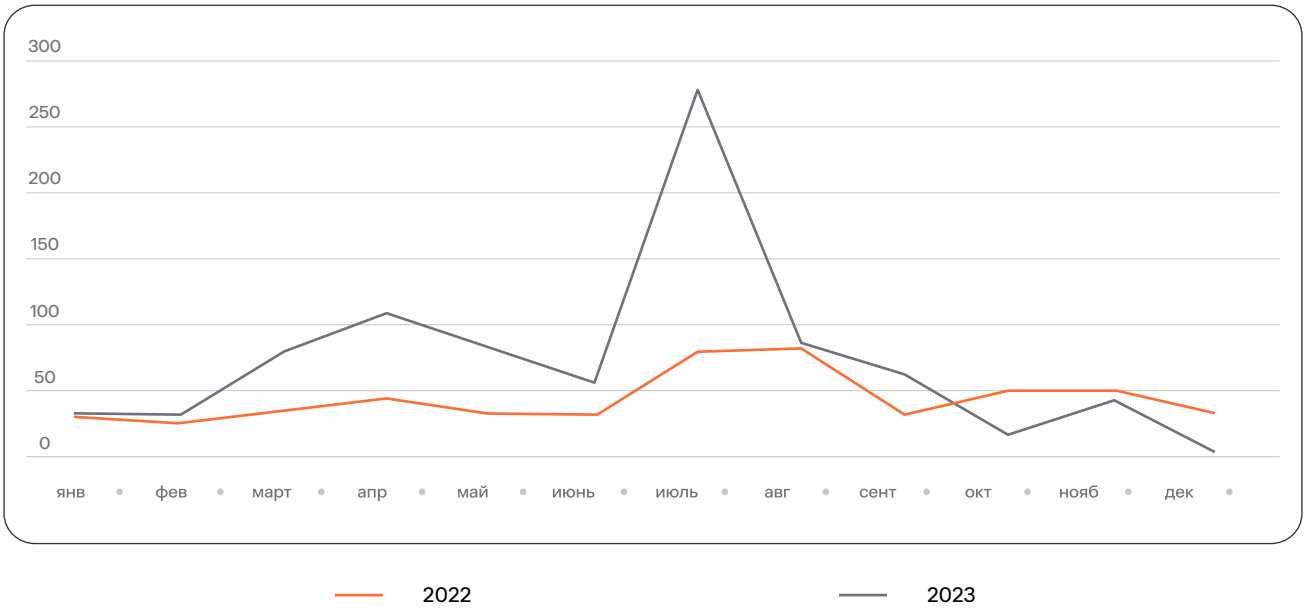


Показатель Mpps важен, так как защита от многих DDoS-атак уровня L3/L4 происходит именно настройкой пороговых значений по количеству пакетов в секунду, особенно в условиях, когда неизвестна величина пакетов в килобайтах.

Атаки с одинаковым количеством пакетов в секунду могут иметь совершенно разный показатель в Гбит/с.

ПРОДОЛЖИТЕЛЬНОСТЬ

Продолжительность DDoS-атак, дни



Средняя продолжительность DDoS-атак в 2023 году существенно снизилась. Тем не менее самая долгая атака в три раза превысила максимальный показатель 2022 года. Она была направлена на регионального интернет-оператора. Снижение длительности атак говорит о том, что хакеры больше не хотят тратить ресурсы на долгий и изматывающий жертву DDoS. Увидев, что нарушить доступность ресурса сложно, они переключаются на другие, менее защищенные цели.

9 МЕСЯЦЕВ

длился самый продолжительный DDoS в 2023 году

ТОП-5 ВЕКТОРОВ АТАК ЗА ГОД НЕ ИЗМЕНИЛИСЬ:

01

TCP ACK

02

SYN-flood

03

UDP-flood

04

Атаки на GRE

05

Атаки фрагментированными пакетами

Большая часть атак осуществлялась по одному и тому же шаблону с применением ботнетов. Это говорит о том, что хакеры фокусируются на проверенных векторах. С одной стороны, они совершенствуют эти методы, увеличивая мощность и охват. С другой – экспертам по Anti-DDoS понятны и известны инструменты защиты.

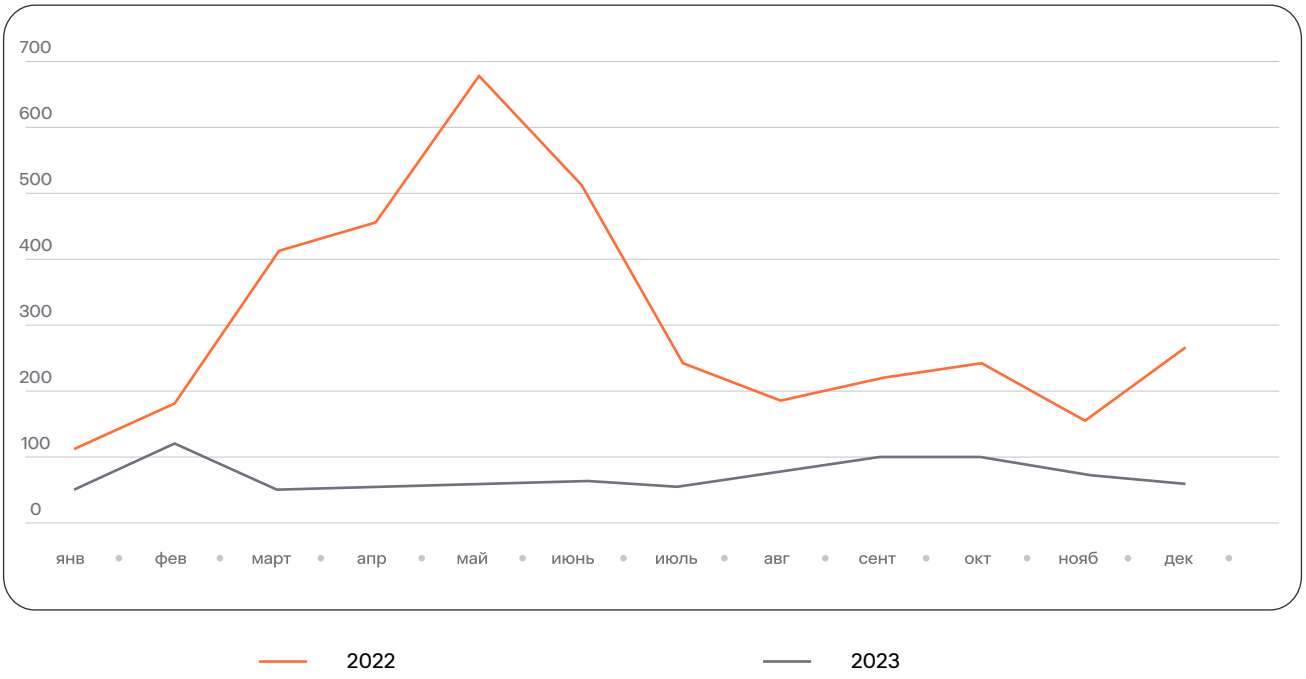
90%

мощных атак приходится на SYN-flood

За год число организаций, столкнувшихся с DDoS-атакам, выросло. Если в первом полугодии атакам подверглось 64% наших клиентов, то во втором полугодии – уже 72%.

При этом злоумышленники стали тратить меньше ресурсов на одну усредненную организацию, но свои усилия они распределяли равномерно в течение 2023 года. Можно предположить, что охватными, но несильными атаками они ищут потенциальную жертву со слабой защитой от DDoS, а после обрушивают на нее мощную атаку.

Распределение атак удельно на одну организацию, шт.



Также мы наблюдаем более равномерное распределение атак по отраслям. То есть сфера деятельности организации уже не имеет такого значения, как раньше, злоумышленникам интересны любые российские компании.

Топ самых атакуемых отраслей выглядит следующим образом:

Топ атакуемых отраслей в 2022 г.

Топ атакуемых отраслей в 2023 г.

[1] Количество DDoS-атак на одну организацию за год.

Интерес к телеком-рынку со стороны хакеров объясняется тем, что вывод из строя ресурсов оператора напрямую отразится на его клиентах, чьи сайты также станут недоступны для пользователей.

Аналогичная ситуация и с ИТ-компаниями. Все чаще они оказывают облачные услуги для клиентов. И если сервис-провайдер не заботится о своей DDoS-защите, то рано или поздно потребители его услуг столкнутся с недоступностью облака. А это приведет к прямым бизнес-потерям.

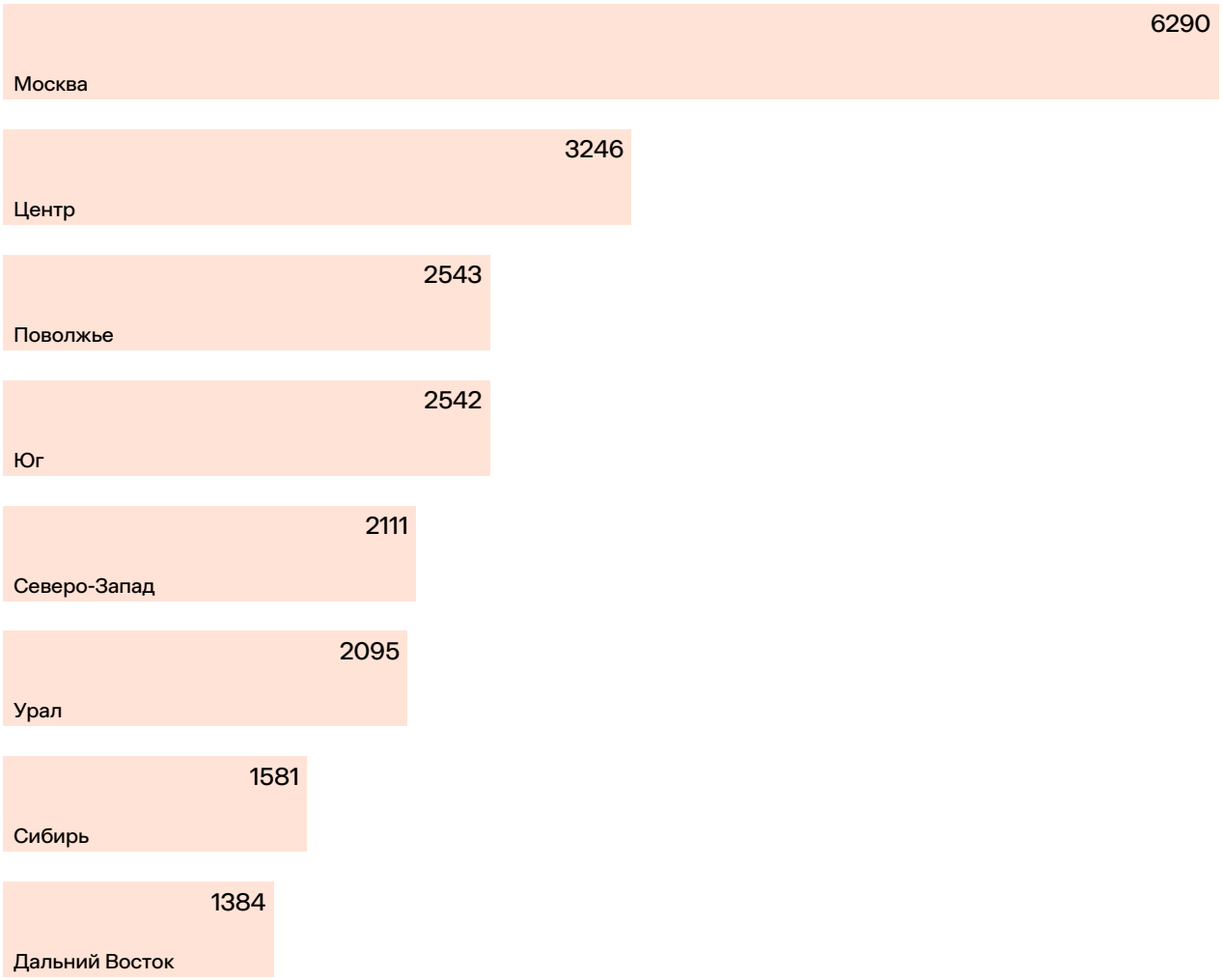
Сервисы доставки и перевозчики также напрямую зависят от своих сайтов, через которые партнеры и конечные пользователи следят за перемещением своих посылок, вносят изменения в условия доставки и т. п.

ГЕОГРАФИЯ АТАК

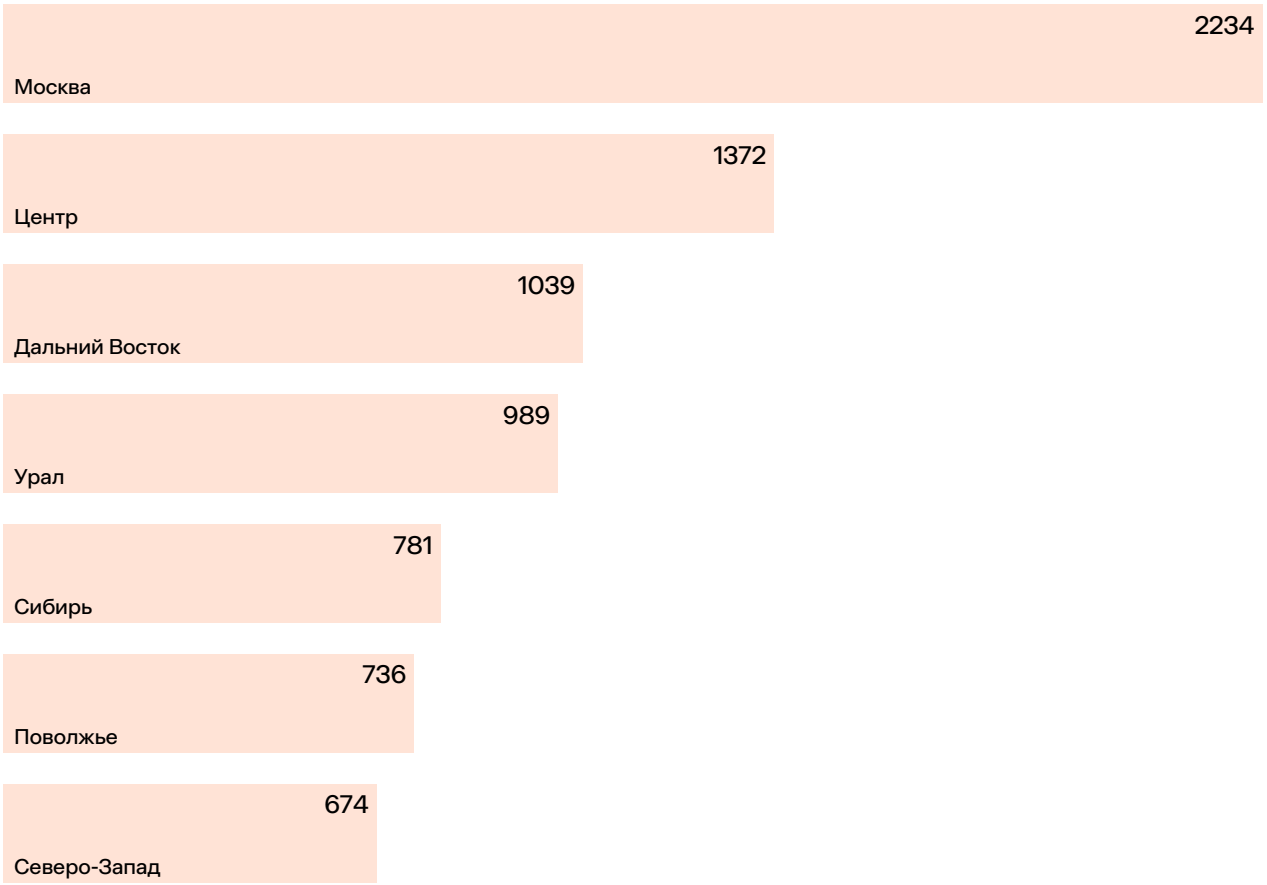
Традиционно наибольшее количество DDoS-атак приходится на Москву, что объясняется высокой концентрацией бизнеса в столице.

Также злоумышленники часто атакуют организации Центрального федерального округа.

Количества атак по регионам в среднем на одну организацию в 2022 году



Количества атак по регионам в среднем на одну организацию в 2023 году



ВЫВОДЫ ПО DDOS-АТАКАМ В 2023 ГОДУ

К концу 2023 года увеличилось среднее количество атак в месяц, выросла их максимальная мощность и количество атакуемых организаций. При этом средняя продолжительность и мощность в конце года упали.

Из этого следует, что злоумышленники перестали фокусироваться на прицельных продолжительных DDoS-атаках и стали наращивать охваты в поисках уязвимых целей (например, компаний, которые не используют защиту от DDoS). При этом максимальная мощность атак растет. На этом фоне ключевым фактором защиты становится возможность провайдера сервиса Anti-DDoS по фильтрации трафика. В частности, сервис Anti-DDoS платформы Solar MSS ГК «Солар» способен отражать атаки мощностью до 5 Тбит/с.

Выход динамики максимальной мощности атак в четвертом квартале 2023 года на уровень 2022 года и новый рекорд в 1 Тбит/с свидетельствуют об усилении возможностей злоумышленников осуществлять мощные целевые атаки и по линии тренда показывает выход злоумышленников на очень высокие уровни мощностей DDoS.

DDoS-атака в случае ее успешности может нанести серьезный удар по организации, например:

- клиенты, не получив доступа к сайту, могут перейти к конкурентам, а сам сайт на время пропадет из поисковой выдачи;
- могут быть атакованы не только публичные ресурсы, но и непубличные, которые используют сотрудники для работы (парализована почта или удаленный доступ к рабочему месту), что приведет к нарушению бизнес-процессов;
- хакеры часто атакуют ресурсы, являющиеся основным инструментом бизнеса, что может привести к серьезным потерям (например, внутренние банковские ресурсы, которые отвечают за транзакции и др.);
- хакеры могут потребовать крупный выкуп, чтобы прекратить DDoS-атаку на сайт жертвы;
- простая DDoS-атака может стать дымовой завесой для более серьезного инцидента, и, пока ИБ-специалисты пытаются восстановить работу сервера, хакеры могут похитить конфиденциальные данные клиентов или корпоративную информацию.

КАКИМИ БЫЛИ ВЕБ-АТАКИ В 2023 ГОДУ

В данной главе описаны атаки, отраженные сервисом защиты веб-приложений (Web Application Firewall, WAF). Веб-атаки направлены на логику самого приложения, когда злоумышленники пытаются использовать уязвимости, которые есть на сайте. Сервис WAF обеспечивает защиту веб-ресурсов заказчика от атак уровня L7 (то есть расширенная защита от DDoS-атак уровня приложений и атак из списка OWASP Top 10, включая SQL-инъекции, межсайтовый скриптинг, незащищенность критичных данных и т. д.)

Одной из ключевых проблем веб-приложений являются устаревшие и уязвимые компоненты программного обеспечения. Можно вспомнить массовые атаки с использованием уязвимостей в CMS Битрикс.

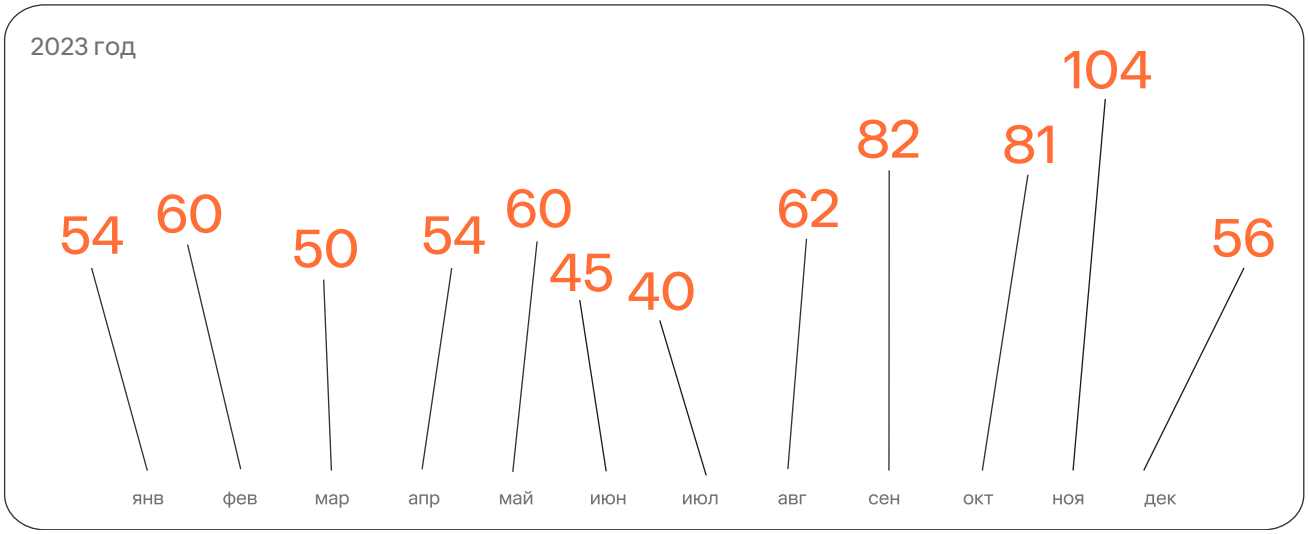
В августе эксперты ГК «Солар» рассказывали про возможности защиты от подобных уязвимостей с помощью Web Application Firewall (WAF), а также про варианты защиты от эксплуатации уязвимостей CMC-сервисов. Все это реализуется на WAF в виде правил, по которым происходит фиксация и блокировка событий ИБ.

Атаки уровня L7 позволяют получить доступ к базам данных приложений, в которых может содержаться персональная информация пользователей. Также есть риск несанкционированного доступа к ключевым функциям системы. В итоге сайт может не открываться, работать медленно или на нем может появиться нелегитимный контент, отпугивающий пользователей или вводящий их в заблуждение (дефейс).

КОЛИЧЕСТВО И ИНТЕНСИВНОСТЬ

В 2023 году сервис WAF зафиксировал почти 750 млн событий ИБ. А крупнейшая L7-атака, отраженная сервисом WAF в 2023 году, составила 300 тыс. RPS.

Динамика веб-атак в 2023 году, млн



На фоне увеличения интенсивности веб-атак сократился средний временной интервал между ними.

Если в начале года этот показатель составлял 614 секунд, то к концу года – уже 168 секунд (в среднем на одном сайте).

ВИДЫ И ПРИОРИТЕТ

Основную долю в 2023 году составляют атаки высокого уровня сложности. В частности, это SQL-инъекции (позволяют внедрить произвольный код в запросы к базам данных), эксплуатация LFI-уязвимостей (позволяют через браузер запускать файлы на сервере) и RCE-уязвимостей (позволяют внедрить вредоносный код в серверную часть приложения). В итоге злоумышленник может получить доступ к управлению веб-приложением и к его данным.

Также в течение 2023 года существенно выросла доля сканирований веб-приложений автоматизированными инструментами. Найденные в результате подобных действий уязвимости позволяют хакерам осуществлять такие веб-атаки, как инъекции.

Блокировка IP-адресов по черным спискам – еще один тип событий ИБ, который часто фиксируется WAF. Процесс автоматизирован, а занесение IP-адреса в черный список происходит на основе составных событий и правил, разработанных с применением экспертизы и опыта команды ГК «Солар».

ПОРТЫ, МЕТОДЫ И СТРАНЫ

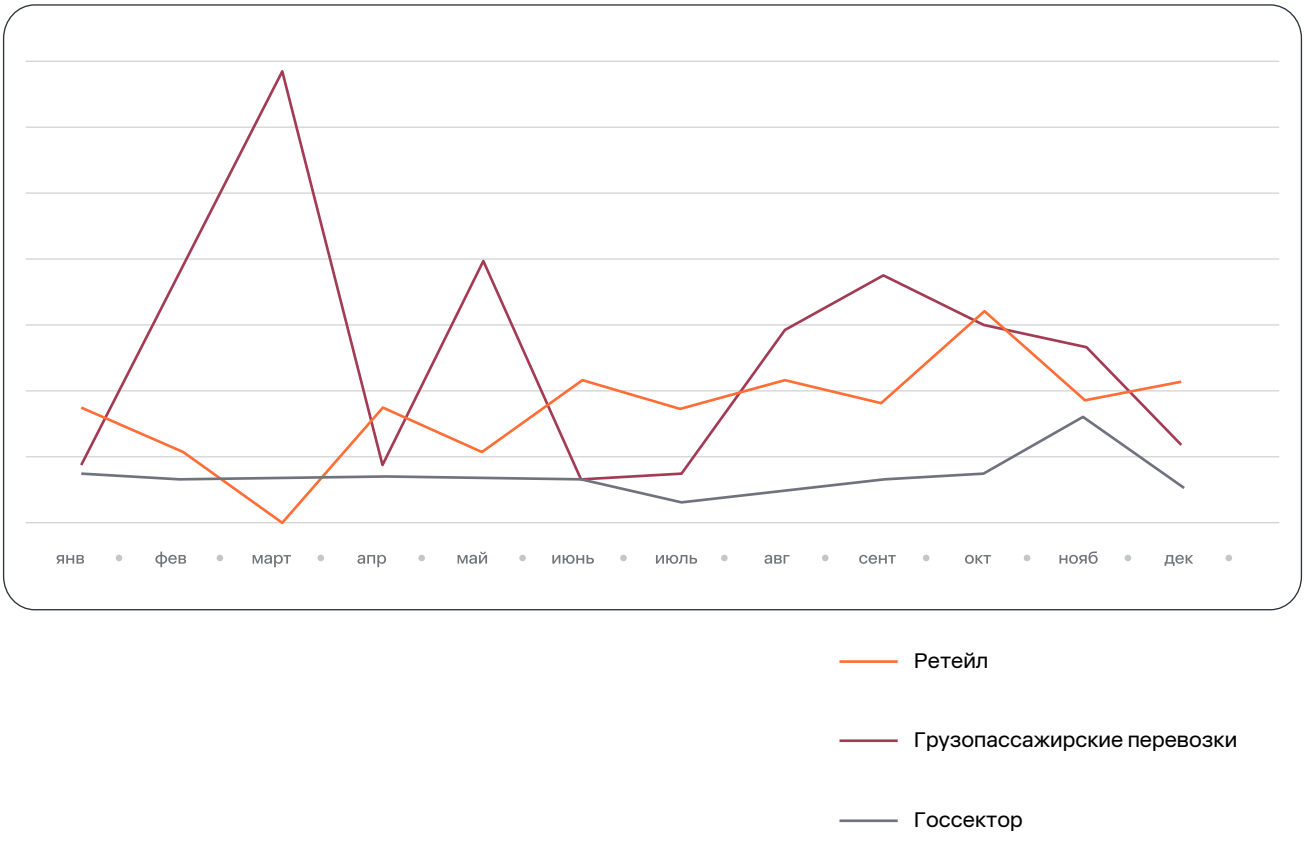
Большую долю веб-атак составляют GET-запросы на 443-й порт (именно на него идет шифрованный трафик HTTPS, который используют почти все организации). Менее 20% атак пришлось на 80-й порт, через который идет нешифрованный трафик.

Большая часть (95%) событий ИБ была вызвана запросами с IP-адресов, находящихся на территории России, что подтверждает тренд перемещения источников атак из-за рубежа на территорию РФ. Это снижает эффективность такого метода защиты, как блокировка IP-адреса по территориальной принадлежности.

Самыми атакуемыми отраслями в 2023 году оказались: ретейл, грузопассажирские перевозки, госсектор. Это отрасли, где большинство клиентов являются физическими лицами (B2C-бизнес), в которых недоступность или взлом сайта напрямую затрагивает конечного пользователя. Также остановка интернет-сайта ретейле и перевозках означает остановку продаж и отток клиентов к конкурентам. А государственный сектор всегда был в фокусе хакеров.

Недоступность общественно значимых ресурсов вызывает панику, так как люди не могут увидеть важную информацию или получить услугу. Дефейс таких порталов вызывает еще и имиджевые потери для госвласти. Кроме этого, веб-уязвимости позволяют злоумышленникам получить доступ к базам данных, в которых может содержаться конфиденциальная информация о гражданах.

Динамика атак на топ-3 отраслей в 2023 году



Злоумышленники увеличивают и концентрируют свои ресурсы на интернет-сайтах. Об этом говорит и рост веб-атак, и числа сканирований веб-приложений, а также большое количество атак высокого уровня сложности. Кроме этого, мы видим, как увеличивается интенсивность веб-атак за счет снижения интервала между событиями ИБ.

В фокусе внимания по-прежнему отрасли, для которых онлайн-сайт является одним из ключевых элементов инфраструктуры и его доступность напрямую влияет на бизнес-процессы. В частности, мы видим стабильный рост атак на интернет-торговлю.

ПОСЛЕДСТВИЯ ВЕБ-АТАК ДЛЯ ВЛАДЕЛЬЦЕВ ИНТЕРНЕТ-САЙТА И ОНЛАЙН-БИЗНЕСА:

01

останавливаются продажи, уменьшается поток выручки;

02

останавливается обслуживание клиентов;

03

у клиентов снижаются показатели удовлетворенности (CSI) и желание рекомендовать ресурсы (NPS);

04

увеличивается отток клиентской базы;

05

снижается LTV, растут расходы на привлечение клиентов для сохранения численности клиентской базы;

06

растут OPEX-/CAPEX-расходы на масштабирование интернет-ресурсов, снижаются OIBDA/EBITDA онлайн-бизнеса.

SOLAR

W: RT-SOLAR.RU
W: RT.RU

Пройти небольшой опрос,
насколько полезной была данная
информация

T +7 (499) 755-07-70
E solar@rt-solar.ru

Центральный офис, 125009, Москва,
Никитский переулок, 7с1