Qrator Labs представила квартальный отчет по DDoS-атакам за 2024 год.

Компания Qrator Labs – это российская компания, специализирующаяся на обеспечении безопасности и стабильности сетей. Она предоставляет решения для защиты от DDoS-атак, мониторинга сетей и управления трафиком. Компания разрабатывает инновационные технологии и предоставляет услуги, которые помогают организациям защищать свои онлайн-ресурсы и обеспечивать надежную работу сетей. Qrator Labs является одним из лидеров в области кибербезопасности и сетевых решений в России и за её пределами, имея офисы в Чехии и Объединённых Арабских Эмиратах." data-html="true" data-original-title="Qrator Labs" >Qrator Labs опубликовала отчет «Обзор DDoS атак по векторам в абсолютных и смешанных значениях» за первый квартал 2024 года. Специалисты усовершенствовали методику сбора данных об интернет-угрозах, сфокусировавшись только на серьезных DDoS-атаках интенсивностью от 1 Гбит/с. Низкоинтенсивные «белые шумы» до 1 Гбит/с были исключены из статистики.

После корректировки методологии картина угроз существенно изменилась. Ранее лидировавший UDP флуд утратил первенство, его показатель составил 24,64%, что на 35,55% меньше по сравнению с предыдущим кварталом. Основным видом атак стал IP фрагментированный флуд, занимающий 40,76% от всех атак.

В общей сложности объем смешанных мультивекторных атак составил 23,22%, что почти в два раза больше показателя предыдущего квартала. Эксперты связывают это в первую очередь с увеличением доступных мощностей. Для опытных хакеров и хактивистов это дает возможность организовывать большое количество атак в виде «ковровых бомбардировок».

Рекордные показатели по длительности и интенсивности атак

Самая продолжительная TCP-атака была зафиксирована в секторе электронной коммерции и длилась 464 часа, или почти три недели. Наиболее интенсивной стала UDP-атака на сегмент онлайн-ставок, достигшая пиковой мощности 881,75 Гбит/с – новый рекорд года. Высокие показатели интенсивности также наблюдались в сегментах интернет-магазинов (686,6 Гбит/с) и хостинговых платформ (270,5 Гбит/с).

Отраслевые тенденции атак

В первом квартале лидером по числу атак (25,26%) стала электронная коммерция. На

втором месте сегмент Финансовых технологий – 22,63%. И на третьем – образовательные технологии – 13,16%.

В статистике микросегментов места распределились следующим образом:

География атак

Что касается географического распределения источников угроз, то тройка лидеров (Топ-20) по числу заблокированных IP-адресов остается неизменной несколько кварталов подряд. Россия вновь возглавила рейтинг с 23,6%, хотя этот показатель почти вдвое ниже, чем в 4 квартале 2023 года (42,03%). На втором и третьем местах расположились США (12,27%) и Китай (7,32%).

Список остальных стран-лидеров также почти не изменился, но их показатели выросли почти вдвое по сравнению с концом прошлого года: Бразилия (4,51%), Германия (4,17%), Сингапур (3,31%), Индия (3,26%), Индонезия (2,96%), Нидерланды (2,69%), Великобритания (2,37%).

Коммерческие атаки набирают популярность благодаря расширению каналов связи, переходу на новые протоколы для удаленной работы и доступности организации DDoS-атак. Количество атак на прикладном уровне L7 снизилось на 22%, что свидетельствует об их более точечном характере из-за высокой стоимости.

Наибольшее число L7-атак пришлось на финтех-сектор (54%), особенно на банки (29,91% всех атак). Зафиксирован рост бот-атак на 18,4%, причем значительная их часть (34,8%) была направлена на сегмент онлайн-ставок из-за повышенного спроса на этот контент. Ожидается дальнейший активный рост числа бот-атак в ближайшие кварталы.

В сфере BGP-угроз существенных всплесков инцидентов не наблюдалось, однако число глобальных утечек маршрутов, затронувших многие страны, удвоилось по сравнению с предыдущим периодом – с 6 до 12 за квартал.