28 марта 2025

Атак не ловит. Почему «карманные» интернет-провайдеры становятся главной мишенью хакеров

В конце марта инфраструктура провайдера Lovit, принадлежащего застройщику ПИК, подверглась массированной DDoS-атаке, в результате которой жители 84 ЖК по всей России остались на три дня без интернета. Для эффективного противодействия таким атакам Роскомнадзор предложил законодательно закрепить требования к устойчивости и живучести сетей связи. Почему искусственное монопольное положение кэптивных провайдеров угрожает качественной и безопасной связи в домах россиян – в материале RSpectr.

РАЗМЕР ИМЕЕТ ЗНАЧЕНИЕ

В связи с многочисленными обращениями и информацией об ограничении доступа к услугам провайдеров для граждан, проживающих в жилых комплексах застройщика ПИК, ФАС России начала проверку жалоб.

В Роскомнадзоре уверены, что для эффективной борьбы с DDoS-атаками требуется доработка законодательной базы. В частности, необходимо

закрепить требования к устойчивости и живучести сетей связи, расширить перечень обязательных мер по защите от DDoS-атак и установить более жесткие требования к резервированию инфраструктуры, считают в ведомстве.

«Противодействие кибернападениям требует ряда мер, от правильного проектирования сети и возможности фильтрации атак на ее границе до использования центров анализа и очистки трафика, а также выстраивания процессов круглосуточной готовности к отражению DDoS-атак», - рассказал RSpectr руководитель центра сервисов кибербезопасности компании RED Security (МТС) Андрей Дугин.

Как отметили в пресс-службе «МегаФона», **схемы хакерских атак не меняются, растет только интенсивность и объем вредоносного трафика.**

Пресс-служба, «МегаФон»: «В 2024 году DDoS-атаки, направленные на интернет-провайдеров, составили примерно 40% от общего числа кибератак, зафиксированных оператором. Хакеры используют именно этот сегмент, чтобы спровоцировать цепную реакцию сбоев и нанести урон большому числу конечных пользователей».

В последние три года «Ростелеком» практически ежедневно сталкивается с масштабными DDoS-атаками, но подразделения кибербезопасности компании успешно их отражают, поделились с RSpectr в пресс-службе провайдера.

Пресс-служба, «Ростелеком»: «В компании выстроена многоуровневая и зарезервированная система борьбы с киберрисками. Причем защита обеспечивается с использованием отечественного ПО и решений».

В «Ростелекоме» уверены, что **одна из причин недавнего массового сбоя – ограничение конкуренции и искусственное монопольное положение кэптивных операторов.**

Директор департамента управления продуктовым портфелем Getmobit Василий Шубин согласен с этим мнением. Этот случай наглядно продемонстрировал риски монополизации рынка, подчеркнул он. Когда есть здоровая конкуренция, провайдер, который хочет выжить на рынке, должен оказывать качественные и безопасные услуги связи.

Василий Шубин, Getmobit: «Целесообразно ужесточить ответственность за вопросы безопасности для провайдеров. Особенно монополистов, пусть даже в ограниченной области».

ДАВАЙТЕ ПОДСЧИТАЕМ

Генеральный директор хостинг-провайдера RUVDS Никита Цаплин рассказал RSpectr, что недавняя DDoS-атака на Lovit в пике оценивалась в 219 Гбит/с. Она сопоставима с крупнейшей атакой на сеть МТС в прошлом году. По его словам, эту атаку можно классифицировать как сверхмощную. Для ее отражения необходимо наличие распределенной фильтрующей сети, чтобы принять атаку как можно ближе к тому месту, где она генерируется.

Никита Цаплин, RUVDS: «Стоимость подобной защиты будет составлять от 2-3 млн рублей в год. Итоговая цена зависит от уровня фильтрации трафика, а также общей полосы трафика, которую нужно предоставить клиентам независимо от того, идет атака или нет».

В случае наложения требований по отражению подобных атак стоимость защиты будет переложена на конечных абонентов и вызовет значительное подорожание услуг со стороны небольших провайдеров, которые ранее не заботились вопросами безопасности своих сетей, отметил эксперт.

Затраты операторов на инфраструктуру будут значительными. Как минимум из-за текущей стоимости оборудования, согласилась ведущий архитектор по информационной безопасности MONS (ГК «КОРУС Консалтинг) Елена Скалозубова.

> С учетом необходимости масштабирования пропускной способности, резервирования критически важных компонентов, внедрения гибридных решений, регулярного обучения персонала и ежегодных апгрейдов итоговая стоимость может достигать десятков или даже сотен миллионов рублей.
>
> Елена Скалозубова,
> Ведущий архитектор по информационной безопасности MONS (ГК «КОРУС Консалтинг)

Желательно, чтобы новые требования регулятора были дифференцированы относительно масштабов бизнеса провайдеров, сообщил директор и основатель ГК K2-9b Group (ГК Softline) Михаил Яненко. Он полагает, что введение единых стандартов для всех может привести к тому, что малые провайдеры «не потянут» высокие затраты, это обернется новыми монополиями.

Михаил Яненко, ГК K2-9b Group: «Оптимально гибкое регулирование, где крупные операторы обязаны соблюдать жесткие нормы, а малые – базовые. В целом предлагаемые меры – это хороший шаг, но даже их реализация не гарантирует полной защиты».

МИНИМИЗАЦИЯ РИСКА

«Ужесточение требований к безопасности операторов связи – это важный шаг, поскольку провайдерские сети часто используются в DDoS-атаках на критическую информационную инфраструктуру», - сообщил RSpectr директор платформы облачной киберзащиты Solar Space ГК «Солар» Артем Избаенков. По его мнению, **многие атаки идут через зараженные устройства в сетях операторов а механизмы их обнаружения и фильтрации не всегда оказываются достаточно эффективными.**

Артем Избаенков, ГК «Солар»: «Мы рекомендуем ввести единые стандарты защиты от DDoS-атак для всех операторов связи, которые включали бы обязательное внедрение современных систем мониторинга и фильтрации трафика».

Введение дополнительных мер господдержки при внедрении отечественных решений по киберзащите может помочь операторам соответствовать новым требованиям, а также повысить уровень безопасности российских сетей, уверен эксперт.

Система оператора связи имеет множество каналов и подключений к другим операторам, а природа маршрутизации трафика асимметрична, то есть трафик к одному и тому же ресурсу в интернете уходит в один канал, а приходит – с другого, рассказал RSpectr директор департамента сетевых

решений STEP LOGIC Евгений Князев.

Евгений Князев, STEP LOGIC: «Поэтому необходимо строить анти-DDoS-систему, состоящую из двух подсистем: для выявления DDoS-атак, которая осуществляет анализ трафика, и для очистки входящего извне трафика. В результате все усилия выливаются в сложный технический проект».

«Среди интернет-провайдеров только 30% имеют анализаторы трафика и чуть более 30% – решения для его фильтрации. Если же говорить о небольших провайдерах, то там защита от DDoS есть у единичных игроков», - отметил в беседе с RSpectr заместитель генерального директора Servicepipe Даниил Щербаков.

«Хотя предложенные регулятором меры направлены на улучшение защиты, их будет недостаточно для обеспечения полной безопасности в будущем», - поделилась с RSpectr инженер-аналитик «Газинформсервис» Екатерина Едемская.

Екатерина Едемская, «Газинформсервис»: «DDoS-атаки становятся все более сложными, и защита только на уровне фильтрации трафика не охватывает все аспекты безопасности. Современные атаки могут использовать различные каналы и методы воздействия, включая атаки на приложения и системы аутентификации».

Для минимизации риска повторения масштабных сбоев в будущем потребуется развитие координационных механизмов между операторами

связи и обмен данными об угрозах в реальном времени (threat intelligence), уверена эксперт. По ее словам, важно учитывать, что атаки могут быть гибридными, с использованием уязвимостей в управлении, цепочках поставок или человеческом факторе.