

# Сергей Лахин (StormWall): В 2023 году поток атак увеличивается

На что обратить внимание при защите банков от DDoS-атак в 2023 году, «Б.О» рассказал Сергей Лахин, коммерческий директор StormWall

Текст

АНАТОЛИЙ ВЕЧКАНОВ,  
ОБОЗРЕВАТЕЛЬ «Б.О»

— Сергей, какие угрозы несут DDoS-атаки банкам в 2023 году и какой ущерб они могут причинить?

— Вот уже больше года продолжают массированные DDoS-атаки на российские организации на фоне сложной политической ситуации в мире. В 2023 году поток атак увеличивается, и ландшафт рисков ИБ заставляет искать более эффективные решения. Больше всего DDoS-атак в этом году направлено именно на российские банки. Большинство атак запускают политически мотивированные хактивисты, постоянно создающие все новые инструменты. Используются масштабные ботнеты для запуска атак мощностью до 1,4 Тбит/с, и это не предел.

— Какие ошибки совершают банки, пытаясь самостоятельно отразить DDoS-атаки?

— Некоторые банки выстраивают защиту своих интернет-приложений, в том числе систем ДБО, «по старинке», не учитывая риски текущей ситуации. Сейчас DDoS-атаки идут на всех уровнях: сетевом (L3), транспортном (L4) и на уровне приложений (L7). Защиты на отдельных уровнях уже может быть недостаточно. Кроме того, защита интернет-сервисов финансовых организаций обладает спецификой: в ряде случаев необходимо применять методы, которые не предполагают раскрытие частных ключей SSL.

— Как правильно организовать DDoS-защиту?

— Прежде всего важно помнить, что для создания эффективной защиты интернет-ресурсов и сервисов банков от DDoS-атак целесообразно применять разные методы защиты, чтобы обеспечить ее эффективность как с точки зрения безопасности и устойчивости, так и экономически — чтобы снизить затраты. Для того чтобы правильно выстроить стратегию защиты, нужно сначала провести аудит ИБ банковских интернет-сервисов с привлечением специализированных компаний, обладающих экспертизой в этой области и большим опытом работы на банковском рынке. В ходе аудита проводятся стресс-тесты банковских сервисов, а также организуются другие проверки на их устойчивость к DDoS-воздействиям.



— Как правильно выбрать провайдера, который сможет обеспечить надежную защиту от DDoS-атак?

— Для этого нужно обратить внимание на несколько особенностей. Во-первых, необходимо выяснить, в течение какого времени компания занимается защитой от DDoS-атак и специализируется ли она на этих сервисах. Особенно важно понять, насколько давно компания занимается защитой именно банков. Во-вторых, нужно узнать, как организована техническая поддержка. Чтобы обеспечить высокую доступность ресурсов банка, она должна работать круглосуточно и без выходных. Преимуществом является наличие нескольких каналов коммуникаций. В-третьих, полезно узнать, какие крупные клиенты есть у провайдера. Количество таких клиентов будет указывать на реальный уровень качества сервиса. Помимо этого желательно протестировать сервис перед его приобретением. И наконец, очень важны затраты. Необходимо выяснить, есть ли у провайдера дополнительные платежи за объем атаки или количество атак. Нельзя соглашаться на такие платежи, поскольку от банка никак не зависит, кто, как и в каком объеме будет его атаковать.

Б.О

реклама