Защита приложений и веб-ресурсов от DDOS атак во время 29-й зимней Универсиады в Красноярске

КЕЙС CORTEL В ОБРАЗОВАНИИ

В период XXIX Всемирной зимней универсиады в Красноярске, заказчик предоставил инфраструктуру для веб-ресурсов мероприятия и столкнулся с резким всплеском попыток информационного вторжения.

Бизнес результат:

Более 10 000 → хакерских атак на веб-ресурсы заказчика было отражено CORTEL за время 29 зимней универсиады в Красноярске.

Доступ 100% → легитимных пользователей к веб-ресурсам заказчика. Работа не прерывалась ни на одну секунду за время универсиады.

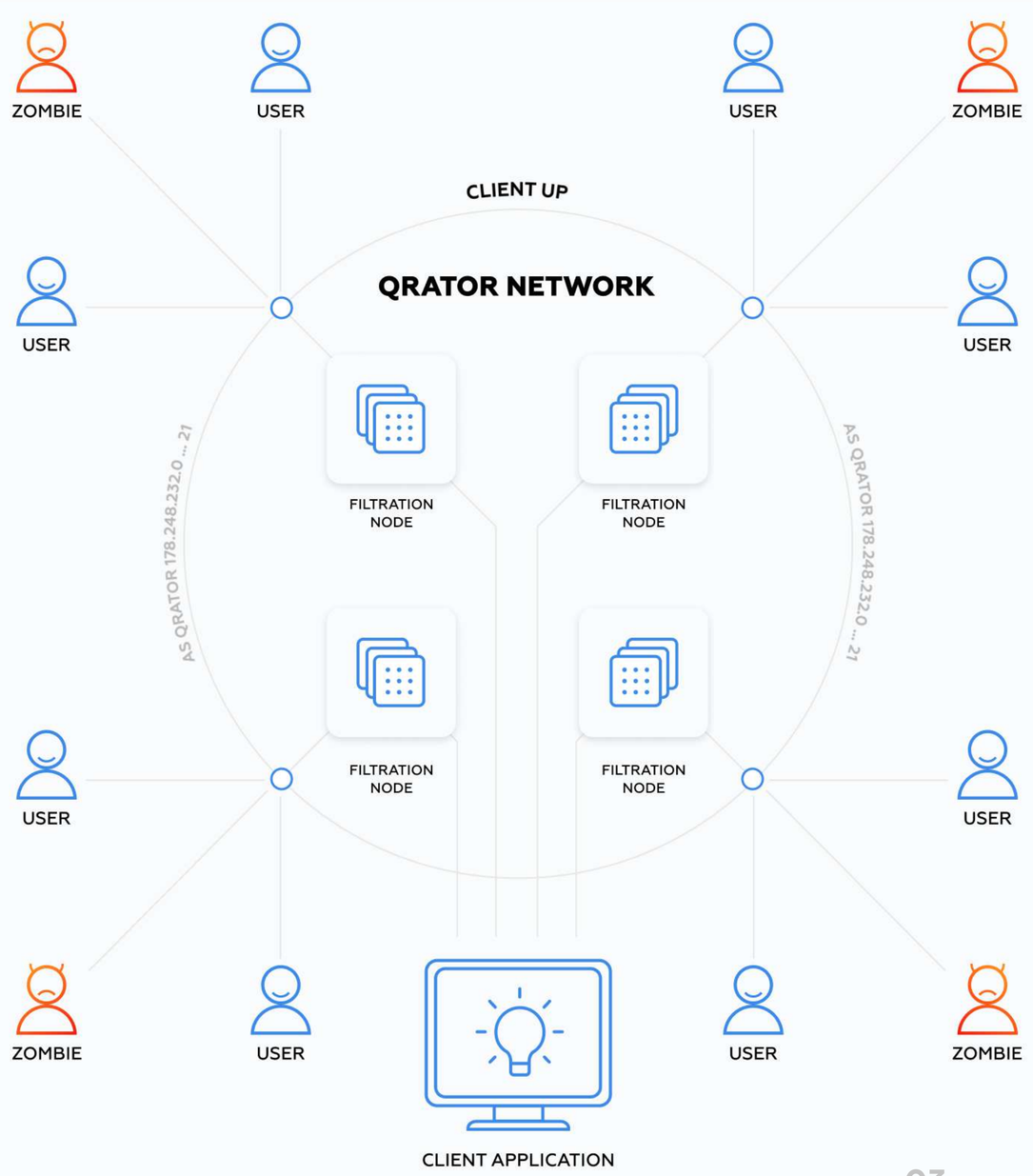
Что было реализовано?

Команда Cortel помогла построить защиту от атак на веб-ресурсы заказчика, расположенные в интернете.

Это стало возможным благодаря внедрению технологии очистки трафика через распределенные центры фильтрации, расположенные на всех континентах.

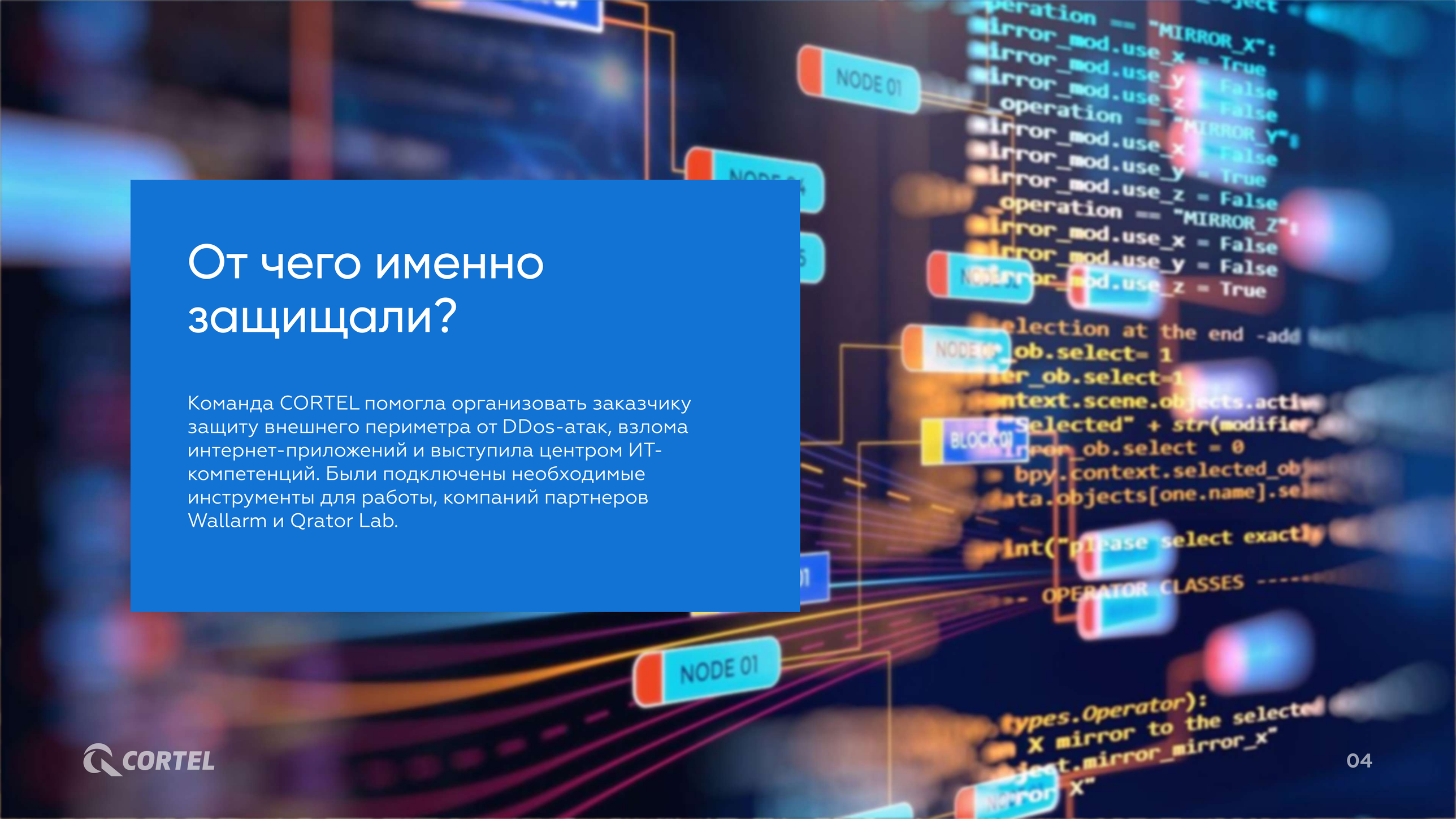
«Большая часть атак пришлась на самое начало студенческих игр: первые инциденты пришлись на ночь с 1 марта на 2 марта. Но наши специалисты были к этому готовы. И сейчас все попытки вторжения успешно отражены. При этом, все легитимные пользователи продолжали свою работу»

- сообщил руководитель отдела кибербезопасности заказчика.



От чего именно защищали?

Команда CORTEL помогла организовать заказчику защиту внешнего периметра от DDos-атак, взлома интернет-приложений и выступила центром ИТ-компетенций. Были подключены необходимые инструменты для работы, компаний партнеров Wallarm и Qrator Lab.



Риски при DDOS-атаках

По данным “Лаборатории Касперского” в 2020 году количество DDoS-атак в России выросло на 223% в сравнении с 2019 годом. По совместным подсчетам аналитической компании B2B International и “Касперского” в среднем убыток от DDoS-атаки составляет около $106 000 США для небольших компаний и более 1,6 млн для крупных корпораций. В отдельных случаях DDoS-атаки обходились компаниям в $160 млн США.

DDoS-атака – это распределенная атака типа «отказ в обслуживании», целью которой является выведения веб-ресурса из строя путем направления постоянного потока запросов с десятков и сотен тысяч зараженных компьютеров, размещённых по всему миру.

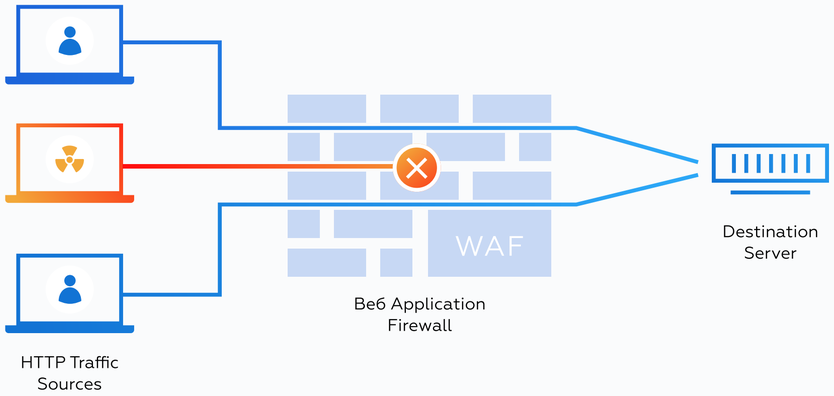
“Какой бы мощной не была инфраструктура, обслуживающая приложения, она не выдержит нагрузку на несколько порядков выше нормы, и выйдет из строя. Это, как правило, приводит к весьма критичным последствиям: потеря репутации или в данном случае - срыву проведения всемирных соревнований”

- отметил технический директор компании Cortel.

Что получил заказчик?

Организован межсетевой экран уровня приложений (Веб application firewall, WAF). Это совокупность мониторов и фильтров, предназначенных для тонкого обнаружения и блокирования уязвимостей.

Технология была реализована через облачный сервис WAF, который не замедляет подключение пользователей к бизнес-приложениям, а для его запуска не требуется обучение сотрудников, отдельная инфраструктура, закупка и установка дорогостоящего оборудования и ПО.



Часто веб-приложения становятся слабым звеном в периметре защиты организации.

Веб-приложения собственной разработки, как правило, обладают сложной архитектурой и множеством заимствованных компонент. Зачастую, разработчики не уделяют должного внимания защите этих элементов

Данные уязвимости становятся основной мишенью злоумышленников и удобной точкой входа для проведения дальнейших атак.

Результаты

ИТ-инфраструктура заказчика защищена от внешних угроз, а 29 универсиада прошла без сбоев из-за атак на веб-ресурсы мероприятия.
Заказчик выразил особую благодарность команде Cortel за проделанную работу и успешную защиту.