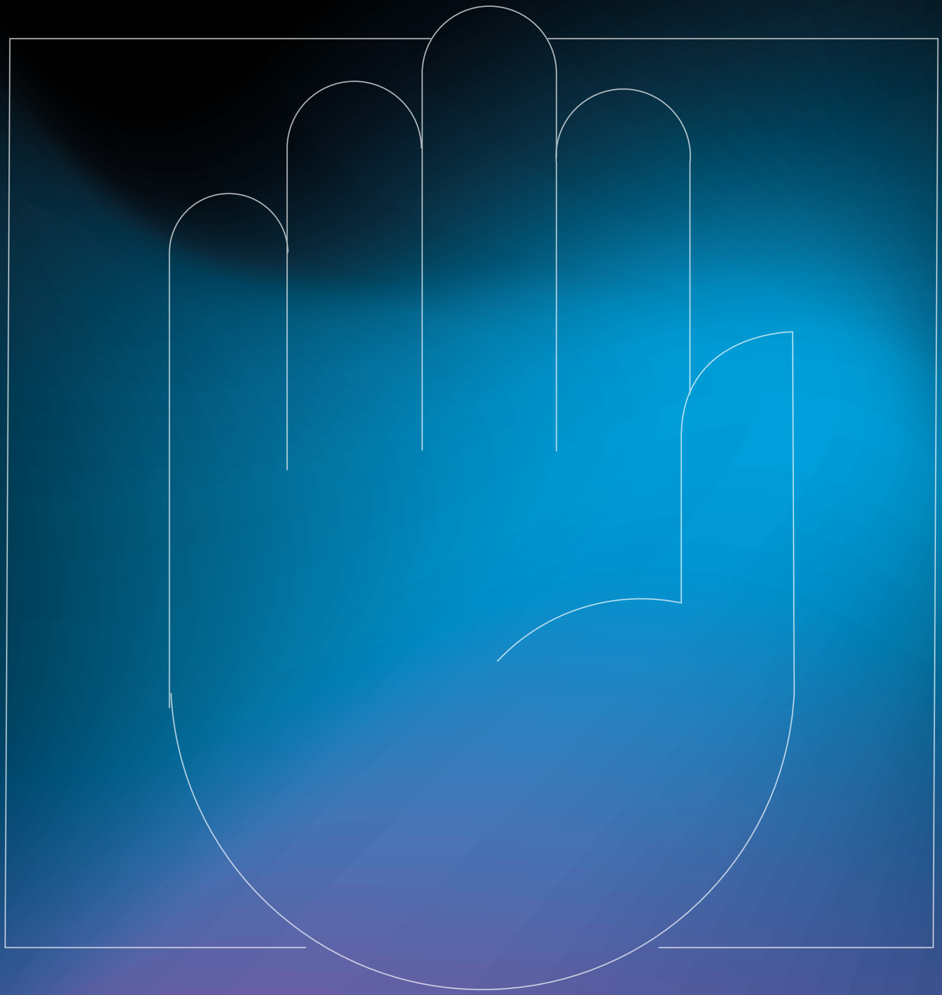
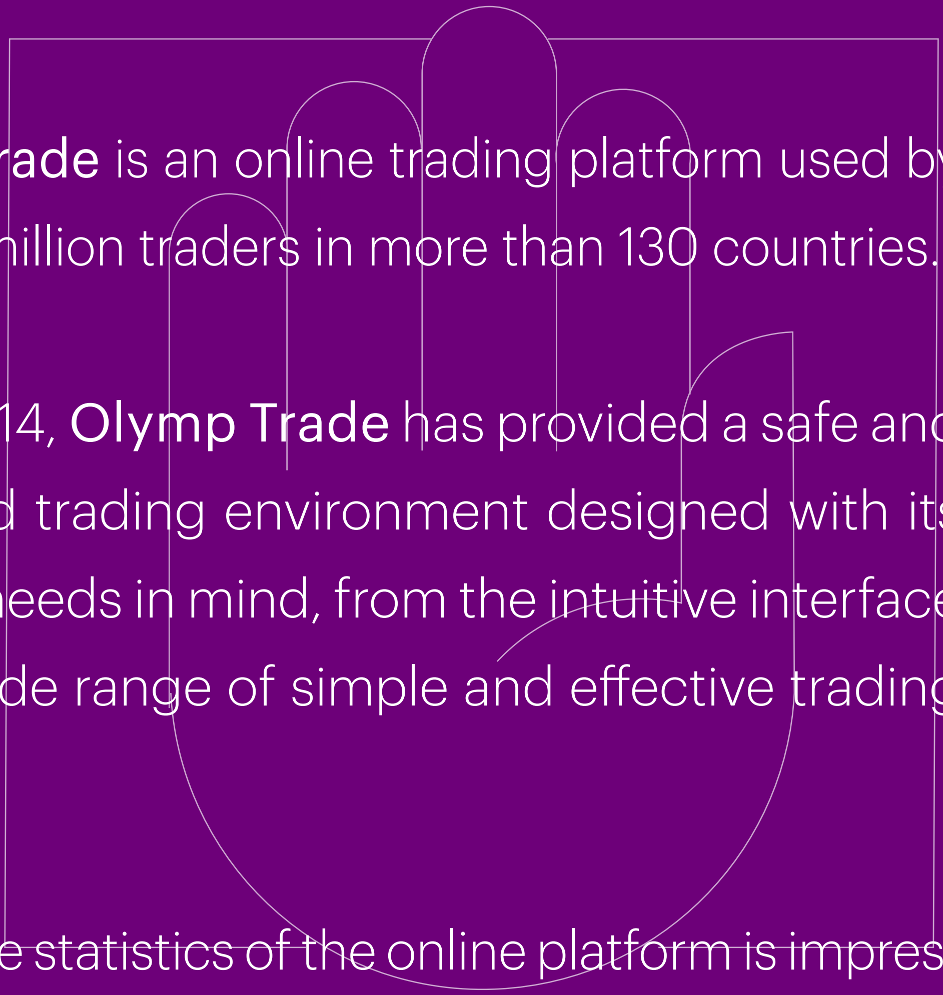
QRATOR LABS

OLYMP TRADE



Use case — Olymp Trade

Olymp Trade ensures availability of its resources and provides a secure trading environment for customers using Qrator Labs filtering network



Olymp Trade is an online trading platform used by over 89 million traders in more than 130 countries.

Since 2014, **Olymp Trade** has provided a safe and regulated trading environment designed with its traders' needs in mind, from the intuitive interface to the wide range of simple and effective trading tools.

The usage statistics of the online platform is impressive: the number of simultaneously trading sellers reaches 20,000, the amount of daily transactions on the platform is over 1M. Moreover, within a month 100,000 new traders make about 15 million transactions.

Challenges

Such a high financial activity on the Internet cannot stay unnoticed, so the issue of possible cyberattacks was hugely urgent for **Olymp Trade**.

Engineers of Olymp Trade note that intruders attempts to hack the system have repeatedly been observed. However, significant negative consequences on the system and critical losses can be avoided through a combination of technical and administrative measures.

For example, by a separation and additional protection of funds circulating in the system: “just like that” you would not be able to withdraw the money. Any withdrawal attempt should receive information from the account holder. Thus, any suspicious activity would be instantly suppressed.

Solution

Olymp Trade considered DDoS mitigation services from several contractors, but, in the end, made the **Qrator Labs** decision. Among the main reasons were a positive teamwork experience, high professionalism and a complete understanding of the internal technical structure of the financial company.

“The effectiveness of the **Qrator Labs** solution is high”, said the **Olymp Trade representative.**

Experience

Crucial moment

Some time ago, **Olymp Trade** first encountered a persistent DDoS attack, the largest in the company's history. Hackers planned to disable the system and start demanding money. Employees received various letters with direct threats and extortion.

"It is fair to admit that we did not immediately realize that the abnormal activity is hiding a real threat", said **Olymp Trade** representative. "By carrying out extensive advertising activity, we already faced a severe increase in requests that put a significant load on the platform, and at first believed that our system does not withstand a large number of new and relevant users. It seemed to us that this traffic was valid until the experts began to disassemble it by logs.

Attempted attacks aimed L2 and L7 on several vectors, starting with trial strikes on our service and ending with a long night series of continuous requests.

Our 24-hours technical support service immediately reported a significant deterioration of service and instability of the platform: at night we raised the team of our technicians and, having evaluated the problem, started switching to the **Qrator Labs** filtering network."

Sometime after connecting, learning and setting up the network, **Qrator Labs** filtered out all the illegitimate traffic, and the work of the platform was normalized.

Experience

Mobile hacking

For the convenience of customers, some mobile applications do not require CAPTCHA input, which malicious actors try to exploit. **Olymp Trade** periodically encounters attempts to compromise end devices and applications, such as brute forcing passwords. The company is aware of such exploitation attempts and actively combats them. To protect customers, new account protection algorithms have been introduced, and a **WAF (Web Application Firewall)** has been adopted to prevent the risk of compromising the trading application.

At the same time, some potential attack vectors are poorly controlled. Infected Android devices redirecting SMS to malicious actors, desktop keyloggers – this is the nowadays reality. Fixing the situation is difficult because this vulnerability exists on the end-user side. We should pay tribute to the **Olymp Trade** technical support specialists, who always warn traders about possible non-market risks and try to find the best options for ensuring their security.

Experience

Olymp Trade notes that not all attack types could be efficiently mitigated by their own efforts — often, it is economically exhausting.

After connecting to the **Qrator Labs** mitigation network, the company's services returned to the normal operation mode. However, this does not mean that the attacks have ceased permanently: massive DDoS attacks have been observed for several weeks. Nevertheless, even after hackers changed their attack vectors, the **Qrator Labs** network quickly adapted to the changes and effectively neutralized new massive requests.

QRATOR LABS

OLYMP TRADE

History of success — Olimp Trade

2023