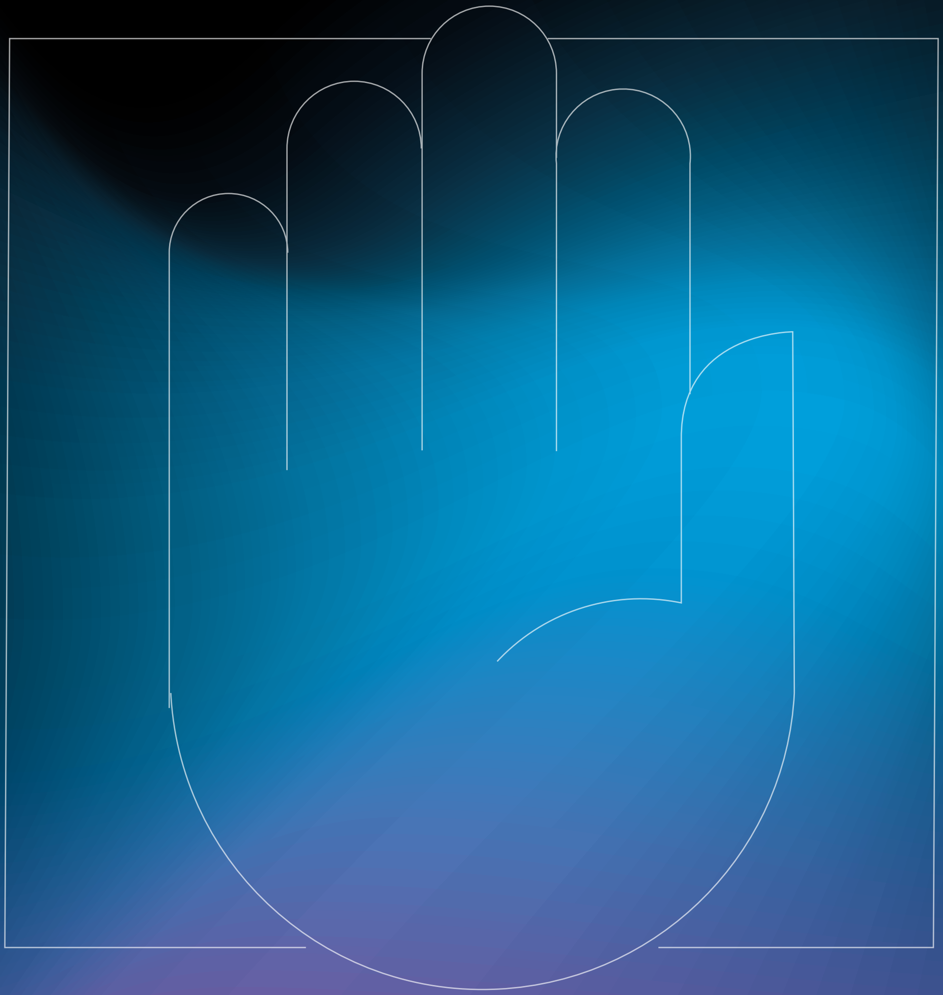
QRATOR LABS



Use case — logistics company

Qrator Labs safeguard a logistics company against Application-layer attacks

Company background

International logistics company, a leader in the fast delivery market, has provided a wide range of goods and cargo delivery services since 2000. Delivery is carried out to more than 67,000 locations in 27 countries worldwide, with the company's representative offices across Europe, the US, APAC, and CIS region. Since 2015, the company has twice been ranked among the Top 5 most profitable franchises according to Forbes magazine. By the end of 2023, the company's revenue exhibited a significant 143% growth compared to the previous year.

The company operates in the B2C segment (delivery of online store purchases), fulfilment (services for online stores and corporate clients, including processing, packaging, storage, delivery, pickup, and returns of parcels), mail forwarding (delivery of purchases from foreign online stores), B2B (document flow between legal entities), C2C (delivery of individuals' parcels), and air cargo (express delivery services) segments.

Use case — logistics company

Challenges

The first half of 2022 saw a massive spike in DDoS attacks targeting logistics companies. Attacks were aimed to disrupt companies' web servers by making them unavailable for legitimate users – a server is bombarded with more requests than it can process.

The logistics sector has never experienced attacks of such volumes before, even though massive cyberattacks have become a new reality nowadays, often leading to disruptions in internal services, difficulties in processing customer orders, and challenges in their shipping and receiving.

It's no wonder that the leading logistics company became a sweet slice of the pie for cybercriminals.

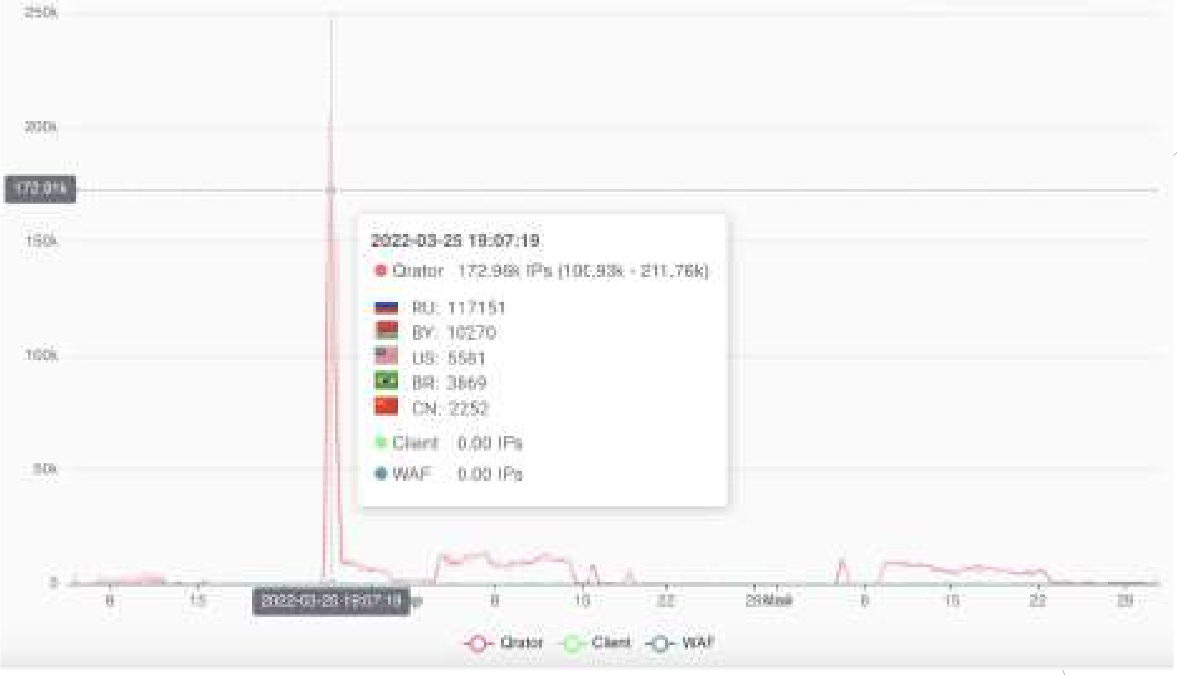
If the company's website is "taken down," all of its business processes will halt, undermining brand reputation and impacting users' loyalty and company revenue.

Solution

After the first waves of attacks, the company decided to avoid the risk of reputational damage and turned to **Qrator Labs** for protection. With the **Qrator Labs** network's total scrubbing capacity, it could filter over 4,000 GB of traffic per second.

But even after **Qrator Labs** set protection and successfully mitigated all the attacks, they were still up and running. Every day, **Qrator Labs** detected a bunch of application-layer attacks. At peak, the **Qrator.Anti-DoS** solution blocked more than 173,000 IP addresses. **The Qrator Labs** network immediately detected and blocked malicious traffic, allowing the protected resource to operate in an ordinary course without service degradation.

Solution



2022-03-25 19:07:19

● Qrator 172.96k IPs (100.93k - 211.76k)

- RU: 117151
- BY: 10270
- US: 5581
- BR: 3869
- CN: 2252

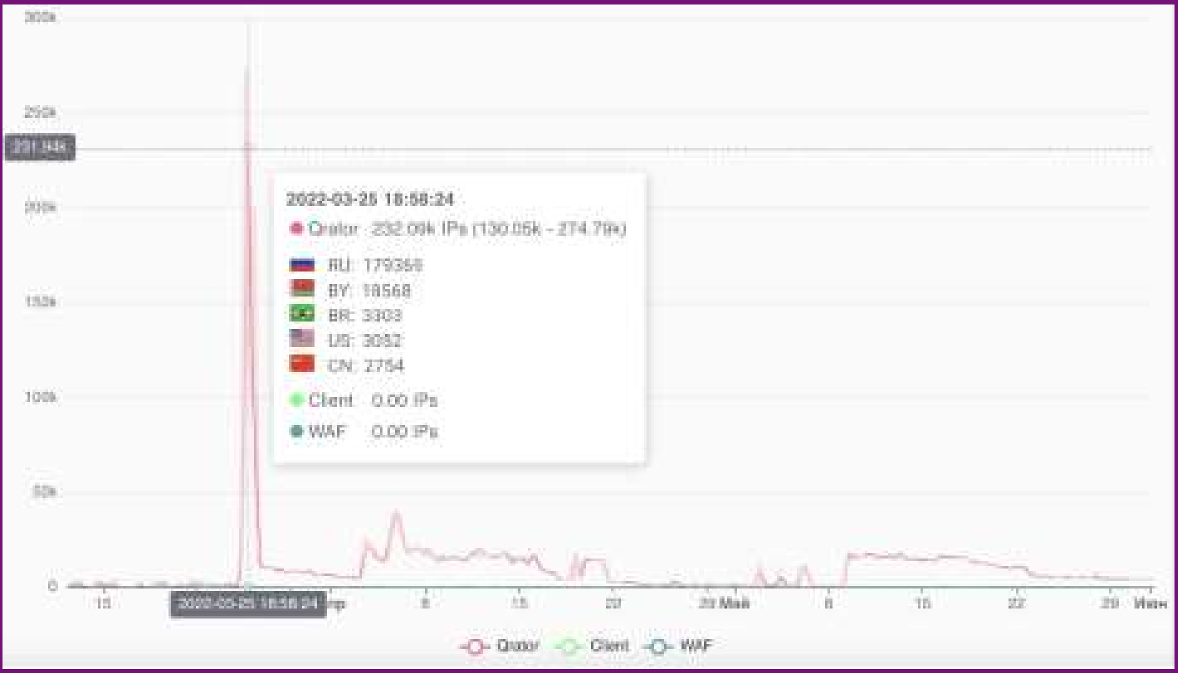
● Client 0.00 IPs

● WAF 0.00 IPs

Additional services of the company were also targeted by malicious traffic – almost 230 000 IP addresses were blacklisted.

Blacklisted IP addresses originated mainly from China, Brazil, Russia, Belarus, the United States, Indonesia, and Germany, as attackers utilized various proxy servers to carry out the attacks.

Solution



The highlights of the attacks:

- ○ The first two quarters of 2022 were the busiest for application-layer attacks
- ○ L7 attacks mimic genuine application traffic
- ○ Application attacks are significantly more challenging and require a large amount of computing power
- ○ Multilayer traffic filtering is needed for the mitigation of L7 attacks
- ○ For detection of any anomalies in the traffic, behavioural, heuristic, and signature algorithms should be used

Solution

"We are happy to help our client neutralize many architecturally complex and non-standard attacks while continuously increasing the power and efficiency of our filtering network to provide businesses with a reliable shield against external threats in today's turbulent cyber environment," commented Victor Zyamzin, global head of business development at Qrator Labs.

QRATOR LABS

Use case — logistics company

2023