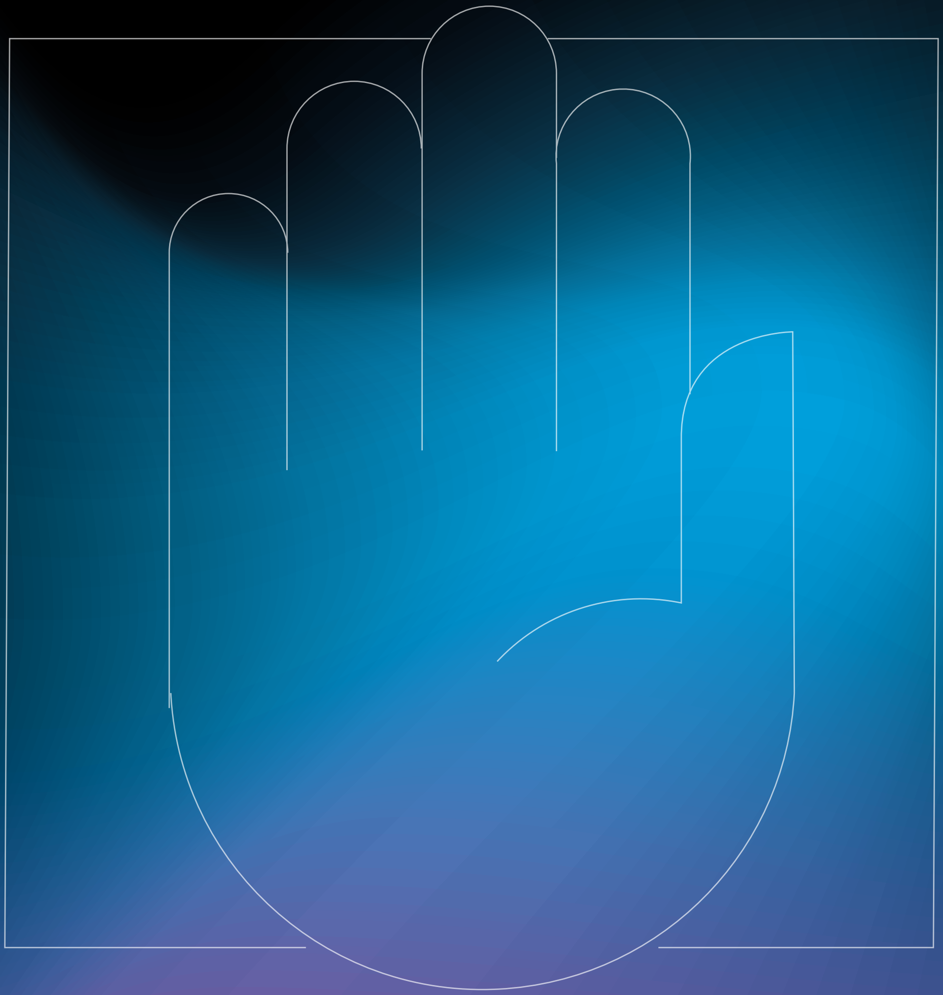
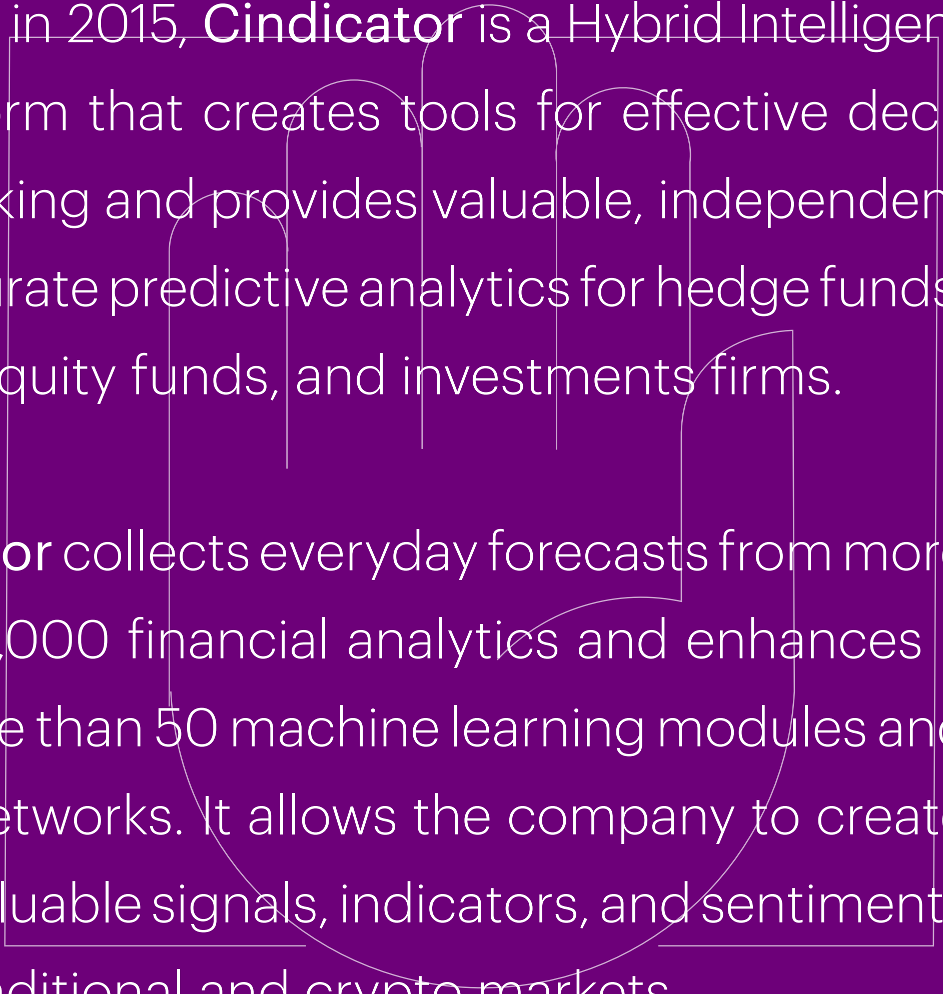
QRATOR LABS CINDICATOR



Use case — Cindicator

Intelligent network attacks protection for competitive trading market



Founded in 2015, **Cindicator** is a Hybrid Intelligence platform that creates tools for effective decision–making and provides valuable, independent and accurate predictive analytics for hedge funds, private equity funds, and investments firms.

Cindicator collects everyday forecasts from more than 130,000 financial analytics and enhances it with more than 50 machine learning modules and neural networks. It allows the company to create highly valuable signals, indicators, and sentiments of the traditional and crypto markets.

Challenges

The high potential of the **Cindicator** project in the scope of rapid cryptocurrencies development makes it very noticeable in the competitive trading market that gives rise of frequently organized DDoS attacks.

Therefore, the company was looking for a **DDoS mitigation** solution that could ensure uninterrupted functioning of its online infrastructure 24/7 thus helping maintain a good business reputation as a reliable service provider.

Solution

After testing a range of solutions provided by various **antiDDoS** providers based on parameters such as SLA, attack response time, global network coverage, price the company preferred the cloud-based filtering service from **Qrator Labs**.

Connecting to the service took only a couple of hours, with no need for any changes to the customer's infrastructure. Currently, **Qrator Labs**' geographically distributed filtering network protects the client's resources from DDoS attacks at all levels of the OSI model, up to the application layer (L7), without requiring the involvement of the customers' specialists and manual configuration.

The platform provides reliable, low latency web infrastructure protection against any cyber threats that could lead to network failure, with 15 points of presence across the globe and filtering bandwidth exceeding 4 Tbps.

Experience

In May 2021, the cryptocurrency market experienced one of its worst days since March 2020. The total market capitalization collapsed by more than $ 500 billion, and the bitcoin rate dropped to $ 30,000 for the first time since the end of January. This rate drop caused a new surge in DDoS attacks.

DDoS attack botnets are also used to mine cryptocurrencies. When cryptocurrencies rates get high attackers redirect botnets powers to mining, which becomes much more profitable. While the decrease in cryptocurrencies rates botnets are monetized in a different way – by arranging commercial DDoS attacks. So, against the backdrop of a cryptocurrencies' sharp collapse on May 25, 2021, **Cindicator** and its product Stoic, a crypto trading artificial intelligence bot, were exposed to two large-scale DDoS attacks, arranged within 2 hours interval.

Experience

The duration of each incident hardly exceeded 15 minutes of continuous malicious traffic. In the first episode, the DDoS bandwidth reached 160 Gbps. It was a low-level flood that was successfully filtered by the **Qrator Labs** network. During the second more serious episode, the attack bandwidth reached 487 Gbps and 47 MPPS, affecting the application layer: the attackers generated more than 8 thousand requests per second to the attacked web application. The filtering system blocked about 4 thousand bots.

Experience

“The safety of Stoic users is our top priority. Connecting to the **Qrator Labs** network has helped **Cindicator** to mitigate infrastructural risks and in the meantime avoid the reputational ones, which is highly important when working with a large number of users. We cannot afford even a single minute of downtime. Our platform must run like clockwork 24/7, and cooperation with **Qrator Labs** helps us reach this continuous availability. The filtering network mitigates DDoS attacks of any complexity in a completely invisible mode, which makes it possible to focus on our business tasks to create a holistic and in-demand traders ecosystem”, comments **Vlad Kazakov, Head of Products at Cindicator**.

QRATOR LABS

CINDICATOR

History of success — Cindicator

2023