GREY WIZARD

GREY WIZARD SHIELD PROTECTS **NOKAUT.PL** SERVICE AGAINST DDoS ATTACKS

CASE STUDY

Nokaut-pl is one of the leaders of the Polish e-commerce market. For many years, for millions of consumers, it is a source of information about the prices of products available in the network, creating one of the most recognisable price comparison engines in Poland. Nokaut.pl is also an independent expert providing current analytical data concerning e-shopping to the general public.

Every year, in the world, there is the increase in DDoS attacks (Distributed Denial of Service). Their target is to paralyse the network infrastructure and application through occupying all the server memory resources and disabling the functioning of the website/service. A properly prepared attack which today most commonly is a distributed attack, and more and more advanced tools used by cybercriminals, may have a catastrophic influence on the operation of services. The effective protection against such attacks is difficult also for the largest entities enjoying great trust.

That was the same in the event of Nokaut.pl

> At Nokaut.pl we have forty servers working for 24h in order to ensure the smooth and trouble-free import of data from e-shops so that customers are able to reach a selected offer easily and quickly - says Marcin Grzybowski, IT Infrastructure Department Head, responsible, for example, for safety at Nokaut.pl.

FIRST ATTACK

On 21 July 2016, the monitoring systems alarmed Nokaut.pl workers that the service is not available to the customers of the price comparison engine and API partners. Servers received so much traffic that protective systems could not rebut such a quantity of inquiries. In one moment all the servers were cut off from the Internet. The team under the management of Marcin Grzybowski took immediate action.

RECENT NOKAUT.PL PROTECTION

> After blocking harmful traffic in boundary routers, Nokaut.pl employees managed to regain the operational access to the infrastructure but during the diagnosing operation on the attack source they received a letter from cybercriminals. – We received an ultimatum – says Marcin Grzybowski

The message was clear. - *We had to transfer a specific amount of money to hackers in exchange for abandoning further attacks. We did not give in to threats but we needed professional help; we were not able to defend against such a serious attack. Our security systems and servers, in the event of DDoS attack, were not sufficient. There were a few prospective security options but in our opinion none of them was effective and fast at implementation* - says Marcin Grzybowski. - *We started to look for a company which would help us resist the attack. A decisive factor to cooperate with Grey Wizard was, among others, immediate website protection, an experienced team of engineers, telephone consultations 24h/7 and a possibility of solution of protecting effectively against similar attacks in the future* - he says.

SECURITY CONNECTION

Connecting to Grey Wizard service is simple and quick. Firstly, it is necessary to provide an IP address which we want to protect. Then we activate a protection service on such an address. In DNS servers we set an IP address of Grey Wizard protecting service and we wait for propagating of addresses in the Internet. It is important so that a prospective attacker is not familiar with the address of our server.

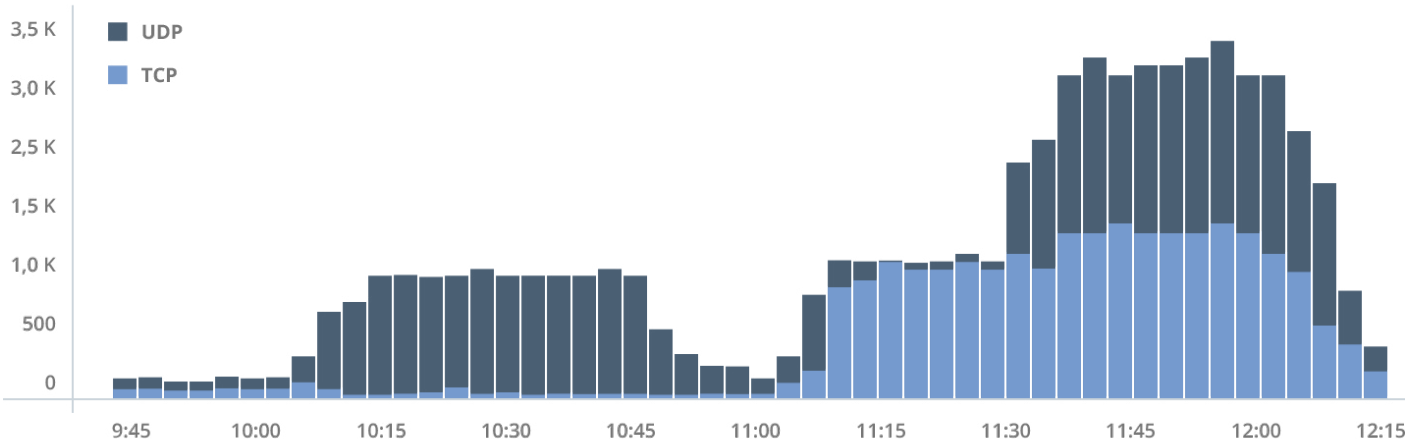
- *A site for managing settings is extended but at the same time very intuitive. It allows for setting many options easily. Yet, what is most important here is that the service is ready for use already with the default settings and you do not have to spend time on it* - says Marcin Grzybowski. - *It is worth mentioning that Grey Wizard engineers provided professional advice during a start-up phase. During an attack they were available 24h* - he says.

GREY WIZARD STARTS ITS OPERATION

The security engineers team from Grey Wizard started preparation for switching traffic and its clearance immediately. After preliminary arrangements with the technical department of Nokaut.pl, the system was ready for intercepting an attack. Nevertheless, a moment before switching the attacked domains, cybercriminals resigned from their action. The situation was again normal but only externally.

On the next day, in the morning, the attack was resumed. The experienced experts from Grey Wizard knew that was going to happen. This is a typical behaviour of criminals. Consecutive attacks and interruptions are to hinder the work of IT department and cause as high financial losses as possible. As the attack was resumed, there was a decision to switch the entire traffic to Grey Wizard.

DDoS attacks are mostly conducted as multi-vector attacks. Every few minutes, attackers change the form of attack. This was the same in this case. The first attack wave is usually volumetric. It consists in



01. Attack methods

blocking a victim's available link. There is also an amplification effect which is the multiplication of an attack through the use of vulnerability in unsecured DNS, NTP servers and CMS applications. Thanks to high capacity links it was possible to resist the attack quickly and ensure immediate protection.

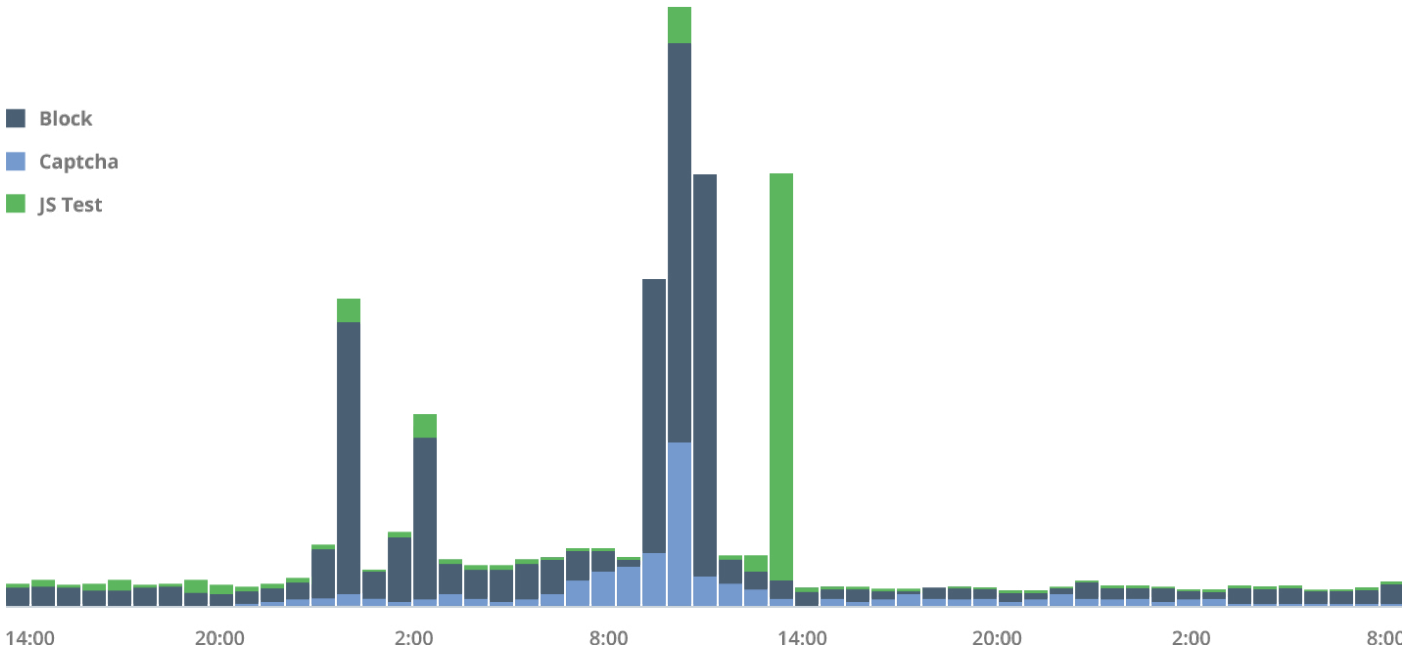
CYBERCRIMINALS' REACTION TO PROTECTION

After a few minutes, criminals became aware that UDP flood attack does not bring the expected results in and they changed an attack vector to SYN flood in combination with spoofing of source addresses. This type of attack consists in the use-up of available processor and server memory resources and rejecting subsequent TCP connections. As a result of an attack, there is an interruption in the access to the server. Thanks to the modern and author's hardware and programming solutions, also in this case, Grey Wizard security was very quick.

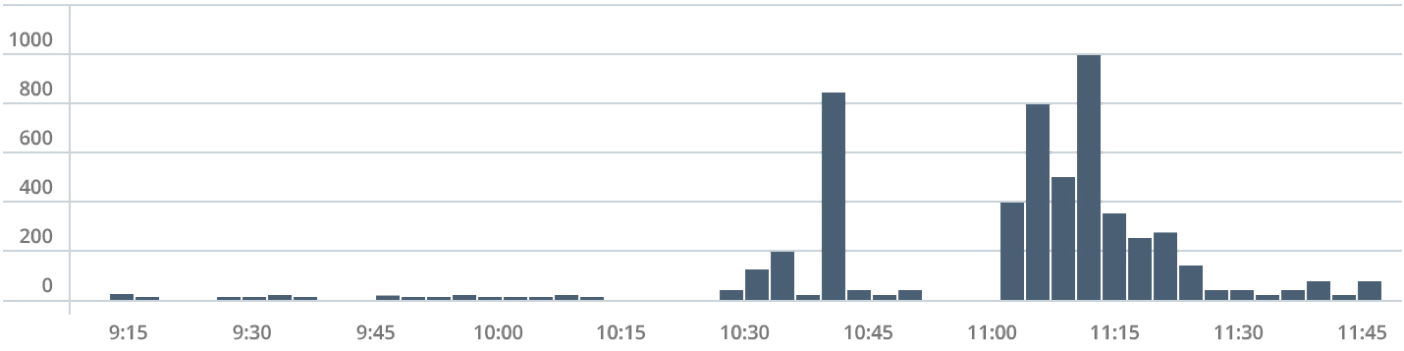
APPLICATION ATTACK VS. ARTIFICIAL INTELLIGENCE

After over a dozen of minutes a form of an attack was changed again. This time it was an application attack consisting in flooding the service with HTTP inquiries. This attack was resisted by means of Web Applications Firewall (WAF) filters and algorithms detecting abnormalities using the elements of artificial intelligence. Within over a dozen of seconds Grey Wizard team was able to isolate a group of IP addresses creating a botnet in the approx. number of 10 000 and use selective blocking so that service users could use it.

For the rest of the day, Grey Wizard engineers observed the re-attempts of attacks. Thanks to the earlier identification of a botnet and precise recognition of attack methods, the response of security systems was instantaneous. Regardless of the layer on which attacks were carried out - they were quickly blocked and there was no impact on the operation of Nokaut.pl. After a few hours, cybercriminals gave up.



02. Anomalies detected by algorithms



03. New attack sources

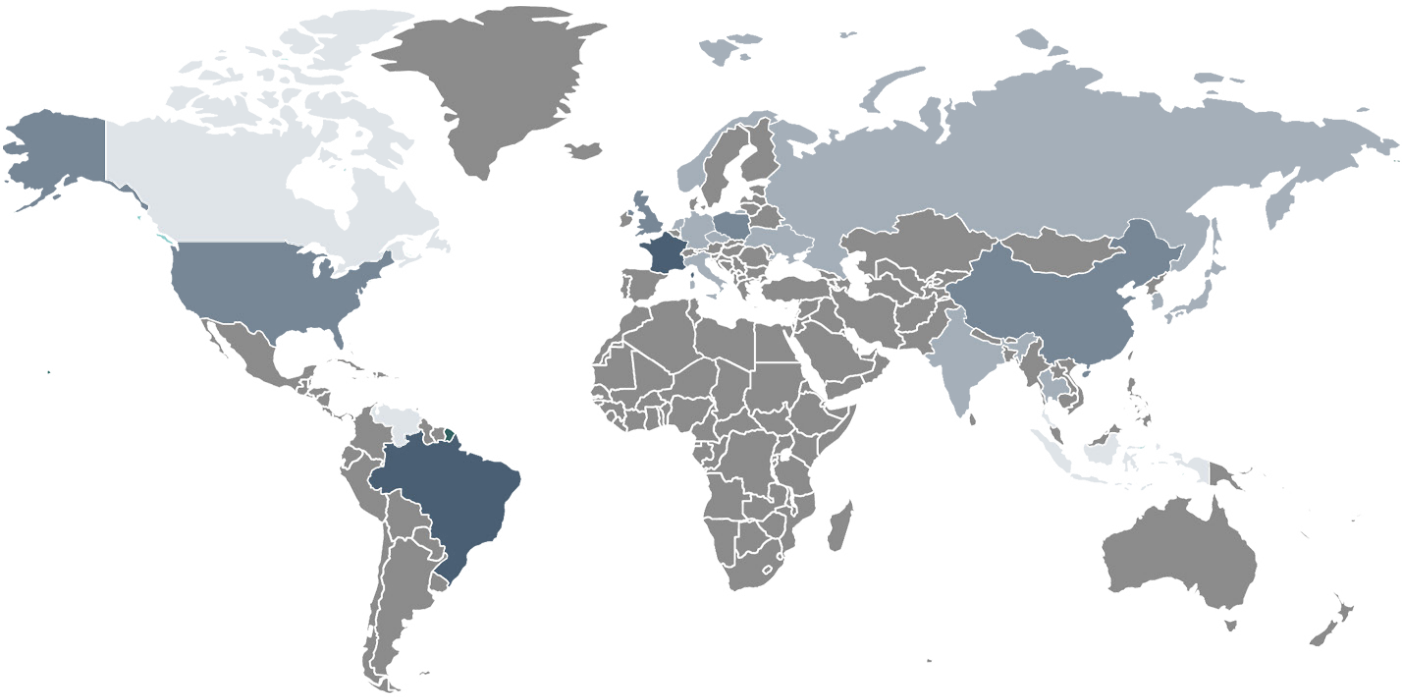
ATTACK CONSEQUENCES

In e-commerce each unavailability of a service is detrimental to incomes, image or reputation. - *Longer unavailability of the service leads to a risk of dropping in the browser ranking. Therefore, it is crucial that the service is available to users and crawlers all the time and responds quickly to each demand* - says Marcin Grzybowski. - *It is also worth mentioning that Nokaut.pl is not only a price comparison engine but also numerous services supporting the e-commerce sector. Owing to the quick response of Grey Wizard engineers, we managed to recover key services. After a few hours, we regained the full availability of Nokaut.pl price comparison engine in the Internet* - he says.

FURTHER COOPERATION WITH GREY WIZARD

From the moment of connecting a protective shield with our services everything works perfect.

In a convenient web panel we are able to introduce minor modifications on our own. This service works as anticipated so we can recommend it with full responsibility. We can always count on express help from Grey Wizard.



04. Map of countries that were the source of traffic to the site at the time of the attack.