GREY WIZARD

GREY WIZARD SHIELDS PROTECT **SMART HOME** TYPE DEVICES

CASE STUDY

Fibar Group SA is an innovative company from Poland acting within the Internet of Things. In six years of starting its activity it has become one of the leading brands worldwide, selling its products on international markets. Fibar Group SA deals in the production and wholesales of FIBARO system elements, which currently is one of the most advanced solutions of building automatics available on the market. Fibaro portfolio includes, among others, such devices as: multi-functional movement, temperature and lighting detectors, flooding sensors or a sensors detecting the opening/closing of any window or door.

FIBARO Home intelligence

- **The global producer of smart home type devices.**
- **The first Polish company which obtained the official Apple certification (products are available at Apple HomeKit platform).**
- **Top data security level** through intelligent Grey Wizard system: WAF and Anti-DDoS, communication coding with the use of TLS protocol and passwords through bcrypt.

HIGH SECURITY STANDARD AS A PRIORITY

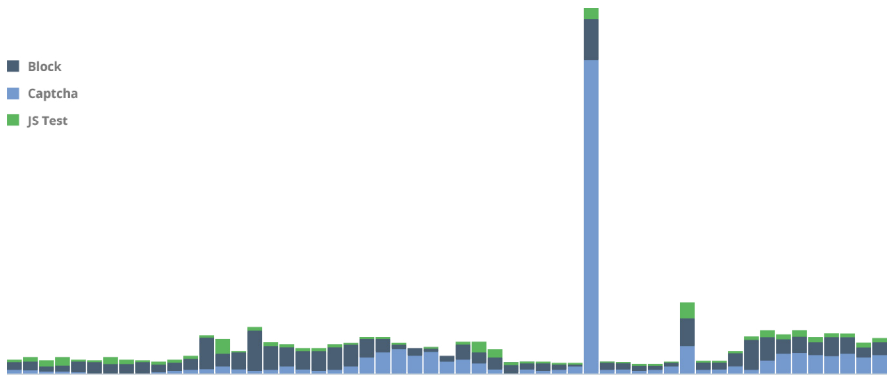
The presence of the company on international markets required a proper technical back-up facility, reliable and efficient IT infrastructure and scalable solutions. Fibar Group satisfied these requirements with flying colours. Yet, there was a threat that along with the dynamic company development and brand recognition increase, there will be the growth in the cyberattack risk. - Fibar is a global company providing access to devices and systems enabling the remote monitoring and managing of smart homes. As it is easy to deduct, taking control over the communication among IT devices and access to their resources may be catastrophic; and in the event of a network attack on the infrastructure, there is a threat of the total blocking of customers from remote service - says Bartosz Nowakowski, responsible for IT security at Fibar Group. - That is why we initiated negotiations with the providers of solutions which will ensure higher security standards and which will protect us against prospective attacks - adds Bartosz Nowakowski.

SMART DEVICES NEED SMART SECURITY

> The main attribute of Grey Wizard is the technological level of the solution itself, its smart functionalities and flexibility – says Bartosz Nowakowski from Fibar Group. - Most suppliers offering systems similar in functionality to the system offered by Grey Wizard has a standardised product which could not be modified for the specificity of our services; and if that would be possible, only within minimal extent which for us is definitely not enough. The invitation of Grey Wizard to collaborate with us was an obvious choice for us - he adds.

THE INTERNET OF THINGS INFRASTRUCTURE DESCRIPTION

The specificity of a traffic generated by Fibaro protected services is not typical. Most commonly, various services are dedicated to a selected group of recipients in a given region, thus it is much quicker to separate the traffic of genuine customers from attack sources. In the case of Fibaro, the situation was much complicated because the recipients of services ale localised worldwide in various time zones. Therefore, the communication means was a hindrance in itself. Communication with Fibaro is mainly based on API and this type of services, contrary to the standard www communication, make use of one http method, and in such conditions it is often hard to notice downloading additional statistical content. This all entails the introduction, with the rules applied so far, of changes adjusting the level of security to the specification of Fibaro services and expectations.



01. Newly detected sources of attacks on API.

CONNECTION OF SECURITY TO GREY WIZARD

- The security activation took not more than 15 minutes. It was very efficient - says Bartosz Nowakowski. - After providing access by Grey Wizard to the account with properly configured security measures, we started switching our services by changing DNS records and deactivating a possibility of direct communication with them - adds Nowakowski. The security in this period acts in a learning mode what allowed us for the detailed verification of the correct functioning of services without the need for blocking any inquiries. After having analysed the operation of security measures and having verified the correct functioning of algorithms active security was enabled.

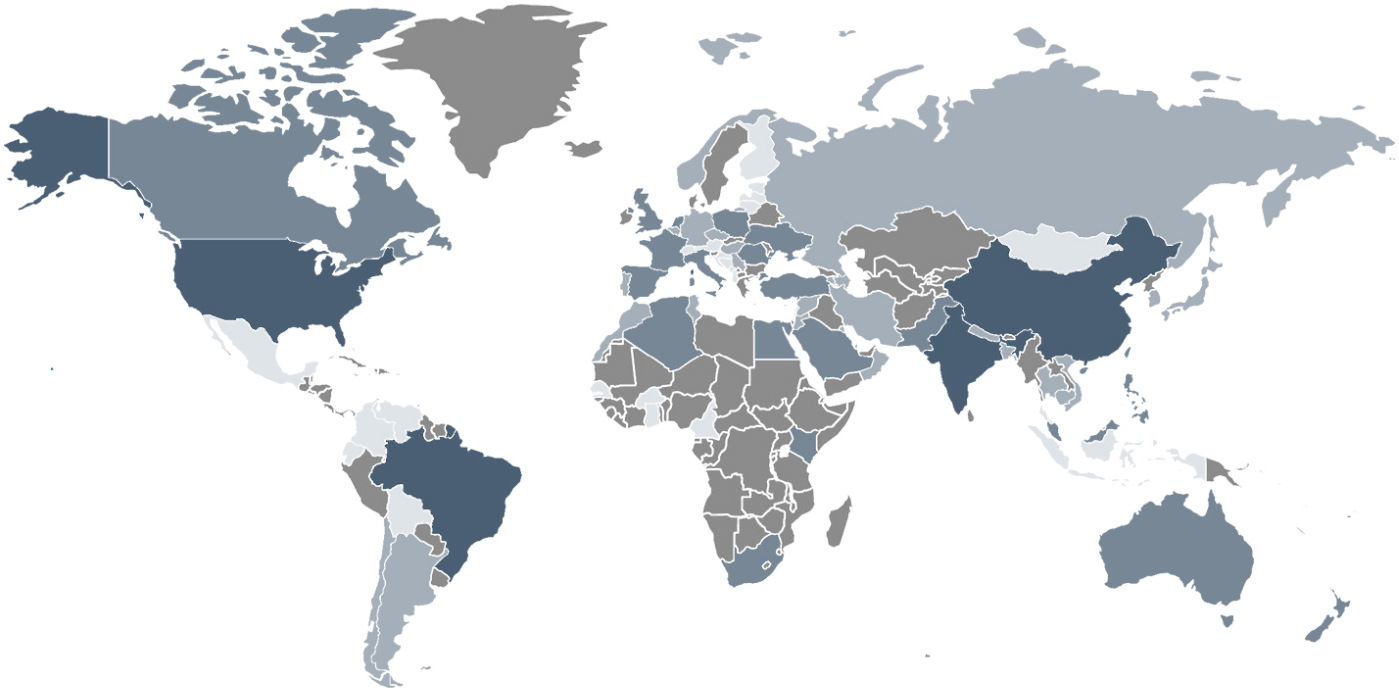
ATTACKS AFTER ENABLING THE SHIELD

The constant monitoring of the functioning of Fibaro services allowed us for detecting malware as part of one of secondary Fibaro websites. The attempts to use this code were immediately blocked. During the analysis, we managed to indicate vulnerability which allowed us for posting a code on Fibaro website and a period within which that incident took place. That was an approximate period because the infection took place a long time before activating Grey Wizard security. Despite this fact, active security enabled detecting that incident.

FURTHER COOPERATION PERSPECTIVE

> At Grey Wizard we were assigned a group of security specialists which is available to us all the time. They are open to our comments and suggestions concerning the system. They adjust the Shield functionalities to the direction in which Fibaro develops. We appreciate it a lot – says Bartosz Nowakowski.

As Fibar Group services develop, Grey Wizard extends its infrastructure and activates subsequent operational points in order to support a given geographical region of the customer's infrastructure. Other data centres will be opened, i.a. in North America, East Asia and Australia.



02. Top 100 countries which are a source of attacks on API.