GREY WIZARD

GREY WIZARD SHIELD PROTECTS **DOBRYMECHANIK.PL** AGAINST STEALING CONTENT

CASE STUDY

dobrymechanik.pl is the largest service with an active base of repair garages with opinions on mechanics in Poland. By means of this website users can choose a verified mechanic, book a repair online and post their opinions after performing the service.

With such a functionality and range, it is important so that the service meets users' expectations and stays equipped with effective protection against cyberattacks.

DobryMechanik
Z nami znajdziesz najlepszego mechanika

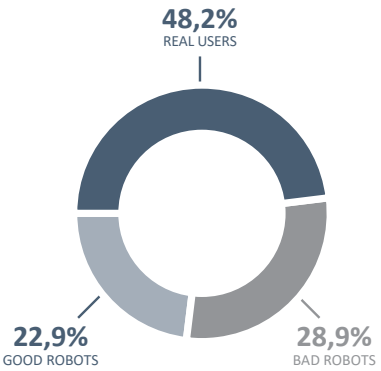
- Opinions on repair garages based in Poland in one place.
- 66 276 issued opinions on 29 504 garages.
- 250 000 of drivers monthly visiting the website.

Protective mechanisms acting at the application level have a great potential. Incapsula BOT Traffic Report 2016 proves that traffic on websites generated by authentic users does not exceed 48.2%, the rest comes from various network tools. Only 22.9% is constituted by "good" robots which scan websites in order to post them in indices of popular browsers, such as Google, Bing, Yahoo or Safari. The remaining 28.9% of traffic is directed at causing specific damage:

- paralysing the functioning of the service,
- stealing an identity,
- gaining access to sensitive data,
- content and other service resources theft,
- collecting e-mail addresses (re-sold to spammers),
- artificial overestimating of the number of visits and clicks which expose advertisers to significant financial losses.

PROBLEMS WITH CONTENT THEFT

Before implementing Grey Wizard security shield, dobrymechanik.pl service had problems with malware which stole content and exploited the Internet link by generating high traffic. There were also attempts of breaking-in which were a serious hazard for the unique content of the service.



01. BOT Raport Traffic 2016: 48,2 proc. web traffic generates authentic users 22,9 proc. it's good robots 28,9 proc. it's the traffic generated by bad robots causing specific damage.

> Such problems usually led to slowing down of the service - says Krzysztof Chudzik, one of the platform creators. - Thanks to Grey Wizard security we got instantaneous protection of our resources and control over undesired traffic. Attacks are effectively blocked both at the application and network level – adds Krzysztof Chudzik.

WAF - EFFECTIVE CONTENT PROTECTION

Web Application Firewall (WAF) is protection at the application level; it is based on statistical formulas and reputation testing mechanisms. It enables monitoring the application in terms of abnormalities and unnatural behaviours of users. Thus, enabling the effective blockade of attempts to scan the entire service in order to steal the content as well as artificial increasing of the statistics of viewing specific subpages.

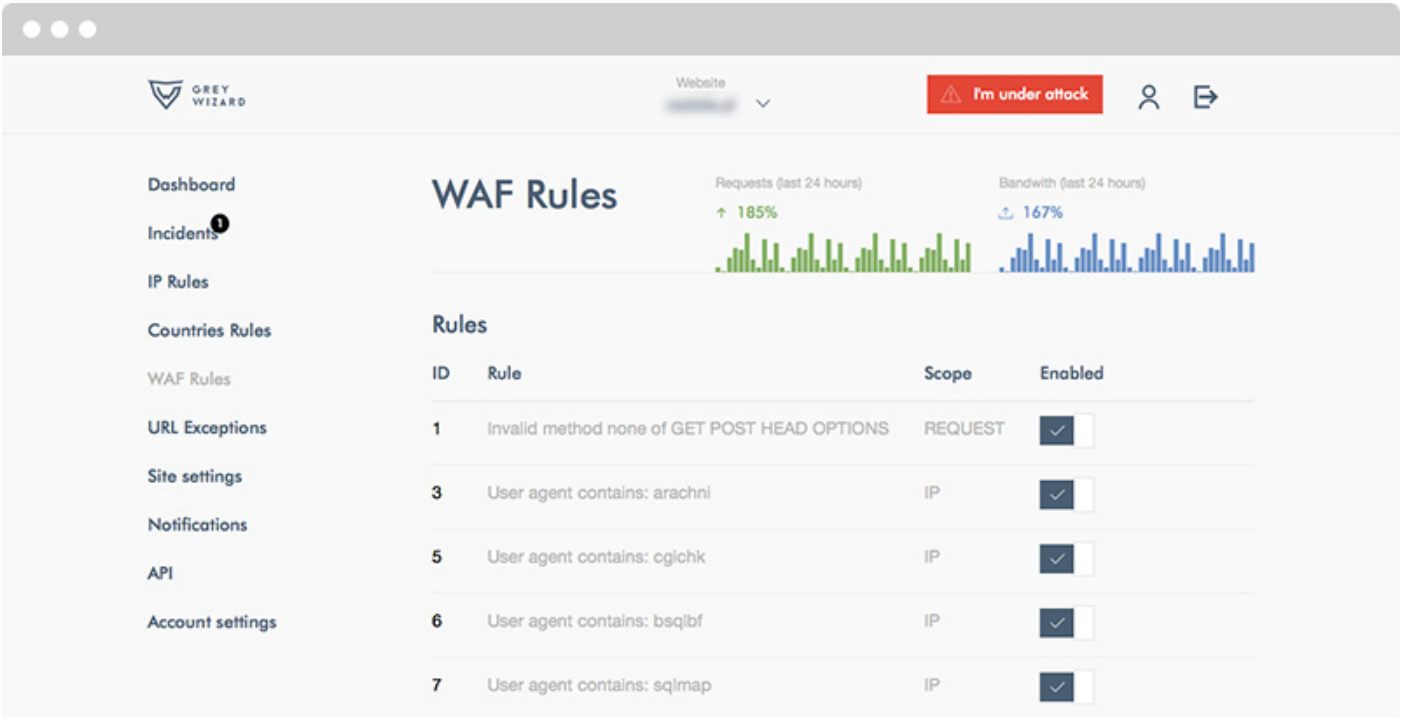
Web Applications Firewall blocks effectively the attempts to scan the entire service for the purpose of stealing the content as well as artificial increasing of statistics of viewing specific subpages.

Grey Wizard shield detects typical network robots, the good ones which are not blocked and robots which scan websites and copy the content (e.g. Scrapy, Butch, Surveybot). So called bad robots are eliminated by means of statistical rules defined by Grey Wizard experts for the needs of a protected service. Such rules are created selectively in order to minimise the frequency of false alarms.

REAL TIME ANALYSIS AND MONITORING

Grey Wizard service protects websites based on the collective knowledge on DDoS hazards, including information on new and more and more popular attacking methods. The intelligent algorithms of machine learning applied in the Shield from the moment of activating protection identify, on a current basis, unwanted traffic, they learn new hazards, and newly detected incidents are stored in the knowledge base.

GREY WIZARD sp. z o.o.
ul. Macieja Palacza 113, 60-273 Poznań



02. Web Application Firewall Rules.

Incidents

IP	Reason	Last action	No. of requests	Details	Actions
64.246.	IP rule: WAF rule: Suspected robots / User agent contains: bad bot (124 rules included)	47 min. ago	1	More	>
216.	IP rule: Grey Wizard behoviour rules (suspicious bot)	58 min. ago	7	More	>
64.246.	IP rule: WAF rule: Suspected robots / User agent contains: bad bot (124 rules included)	1 hours ago	1	More	>
35.193.	IP rule: WAF rule: Security vulnerability scanners / User agent contains: security scanner (64 rules included)	2 hours ago	7	More	>
36.	WAF rule: Software crawlers / Crawler Scrapy	2 hours ago	1	More	>
91.	IP rule: WAF rule: Suspected robots / User agent contains: bad bot (124 rules included)	3 hours ago	1	More	>
94.	WAF rule: Security vulnerability scanners / User agent contains: security scanner (64 rules included)	3 hours ago	1	More	>
64.246.	WAF rule: Suspected robots / User agent contains: bad bot (124 rules included)	4 hours ago	1	More	>
185.85.	WAF rule: Wordpress / Brute force wp-login.php	4 hours ago	1	More	>
185.	WAF rule: Wordpress / Brute force wp-login.php	5 hours ago	1	More	>

03. A panel presenting the newest incidents of security.

Real time analysis allows a user to observe the most important data concerning a website, track current traffic statistics and detected hazards as well as analyse details referring to a given incident.

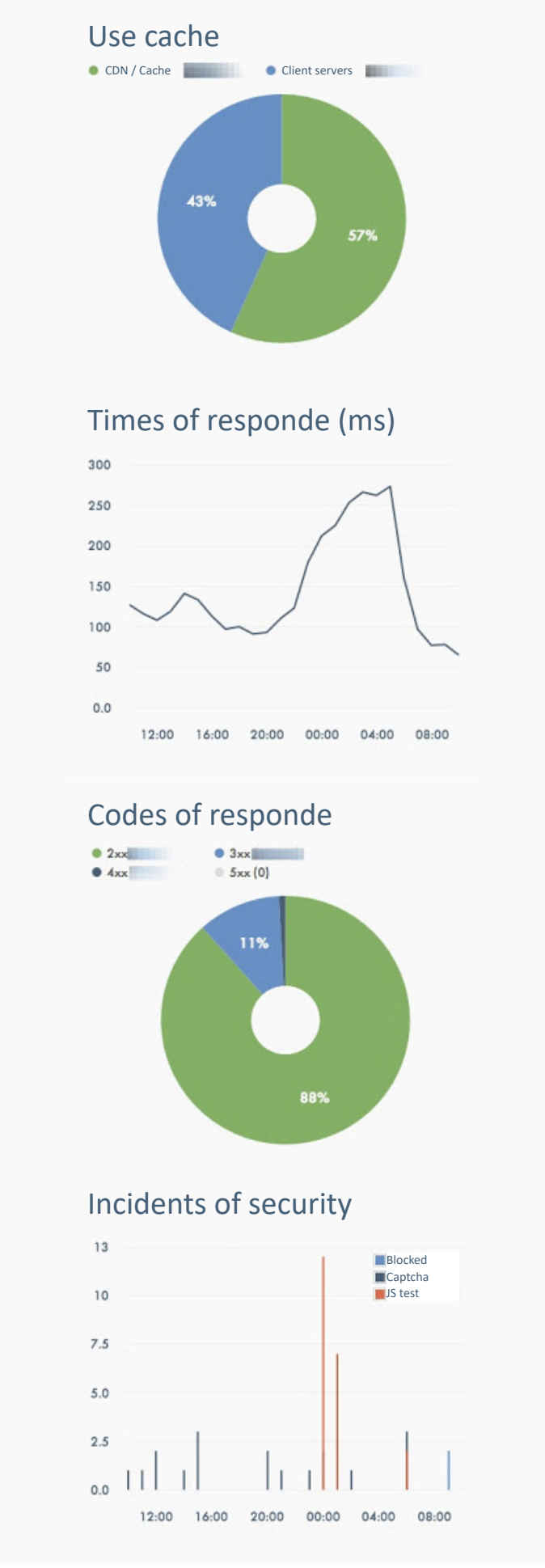
PROTECTION CONNECTION

The activation of Grey Wizard Shield is fast and simple.

> The service installation and configuration lasted a few minutes - says Krzysztof Chudzik. - It did not require any additional hardware or introducing any changes to the application. We only had to introduce IP addresses received from Grey Wizard to DNS settings. Within a few minutes from connecting the protection, we could view first statistics of the website - he says.

FURTHER COOPERATION

> The activation of Grey Wizard Protection Shield allows us to stay calm although there are more and more cyberattacks. This service is performed on a continuous basis, effectively protecting our website against known attacks but also against new prospective hazards - says Krzysztof Chudzik. - Grey Wizards experts are available to us at any time. We trust them completely. They share their knowledge and we make use of it eagerly, implementing their recommendations - he says.



04. An example of a panel with statistics in the real time mode.