Table of Contents

General Description 3

General Description

To carry out a DDoS attack, an attacker has at their disposal a large network of remotely controlled computers (BOTNET), so there is no longer a need to hide the IP address of each individual device (of course, a BOTNET can also be used to amplify regular DoS attacks). In this case, the attacker can simply mimic the actions of legitimate site users, but due to the large number of computers involved in the attack (sometimes hundreds of thousands), even such actions will generate heavy load on the site and lead to a denial of service. Typically, attackers select the most resource-intensive requests to the target site in order to minimize the number of participating computers whose IP addresses might be exposed after the attack.

Various behavioral strategies are often applied to mitigate such attacks with varying degrees of effectiveness, allowing deviations from normal behavior to be detected. Our approach is simple yet very effective — using a CAPTCHA page (Completely Automated Public Turing test to tell Computers and Humans Apart) — a computer test used to determine whether a user is human or a bot.

The protection works as follows:

1. When a threshold value is exceeded, e.g., a comfortable number of requests per second for the site, the protection is activated.
2. Only users on the whitelist are allowed to interact with the site; all others are redirected to a CAPTCHA page to verify "humanness". This page is hosted on a separate server capable of handling a BOTNET of any size.
3. Users who successfully pass the test are added to the whitelist, and their further interaction with the site is uninterrupted.
4. Users who fail the test (bots) cannot proceed past the detection page and cannot generate any load on the targeted site.