Table of Contents

General description 3

General description

A hacker possesses a large network of remotely controlled computers (BOTNET) in order to perform DDoS attack. There is no need to hide IP addresses of these computers[1)]. The hacker can just imitate legit users' activity. However, due to the large number of computers used for the attack (up to hundreds thousands sometimes), this activity overloads the site and leads to the denial of service. Hackers typically employ the heaviest requests to the site under attack. This reduces the number of computers used for the attack. The IP addresses of these computers will be known after the attack.

Various behavioural strategies are used to protect against these attacks. These approaches allow to detect abnormal behaviour and may be more or less effective. We offer a simple and reliable approach: use a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) page. This test allows to define if the user is a human.

The protection works as follows:

1. The protection is trigged by exceeding the threshold value, for example, a comfortable (for a site) number of requests per second.
2. Only those users that are in "white" list are allowed to use the site. All the others are redirected to CAPTCHA page to prove they are humans. This page is hosted by a separate server that can take a load from BOTNET of any size. (One can use the company's server.)
3. Users who pass the test are added to "white" list. They can further use the site in a comfortable way.
4. Users that did not pass the test (BOTs) are unable to get beyond the test page and make any load to the site under attack.

1)

Sure BOTNET can be used to enforce ordinary DoS attacks