Содержание

1 Общее описание

Для осуществления DDoS атаки злоумышленник имеет в распоряжении большую сеть удаленно управляемых компьютеров (BOTNET) и ему уже нет необходимости скрывать IP-адрес каждого из них [1] В этом случае злоумышленник может просто имитировать действия легитимных пользователей сайта, но благодаря большому количеству участвующих в атаке компьютеров (иногда сотен тысяч), даже такие действия вызовут большую нагрузку на сайт и приведут к отказу в обслуживании. Обычно злоумышленники выбирают для вызова наиболее ресурсоемкие запросы к атакуемому сайту, чтобы минимизировать число участвующих в атаке компьютеров, IP адреса которых будут после атаки засвечены.

Часто для защиты от подобных атак с разной степенью эффективности применяются различные поведенческие стратегии, которые позволяют определить отклонения в нормальном поведении. Мы же предлагаем простой и очень эффективный подход - использование странички с CAPTCHA (от англ. Completely Automated Public Turing test to tell Computers and Humans Apart) — компьютерным тестом, используемый для того, чтобы определить, кем является пользователь системы: человеком или компьютером.

Защита работает следующим образом:

1. при превышении порогового значения, например, комфортного для сайта количества запросов в секунду, активируется защита
2. к работе с сайтом допускаются только пользователи, находящиеся в белом списке, все остальные перенаправляются на страничку с CAPTCHA для проверки на "человечность". Эта страничка расположена на отдельном сервере, способном выдержать нагрузку BOTNET любого размера.
3. пользователи, успешно прошедшие тест, добавляются в белый список и дальнейшая их работа с сайтом ни чем не омрачена
4. пользователи, не прошедшие тест (BOTы), не могут продвинуться дальше детектирующей странички и создать какую-либо нагрузку на атакуемый сайт

[1]
конечно BOTNET может использоваться и для усиления обычных DoS атак