1. Отдаём ботам мыла для верификации. Конечно же те которые уже имеют статус «BAD» не отдаём. И получаем все данные для анализа от ботов.
2. Анализируем ответы от ботов. Конкретно Last Response и в зависимости от значения этого поля, выставляем статус. Подробнее ниже.

Теперь подробнее о 3 и 4 пункте.

Отдача инфы ботам происходит по тому же принципу что и смтп. Нужен пул для работы с ботами и так далее. Формат данных для того чтобы отдавать ботам следующий

Параметры:

**6** – команда на вериф мыл

**Количество потоков** – выставляем в настройках верифа мыл

**PTR Record** – это PTR Record для каждого бота своя

**Mailfrom** – прописывается на страничке настроек мыл

**Dns** – список днс через таб, тоже вписывается в настройках

**Email** – мыла, через таб

Для того чтобы были более менее корректные результаты верификации мыл нужно выбрать подходящих ботов. ИП каждого бота необходимо проверить на PTR record, это что то вроде хостнейма. Нам подходят только те боты которые имеют домен в PTR.

Допустим ип 115.76.98.89 имеет PTR: adsl.viettel.vn

113.163.148.138 - No ptr Records exist

Кроме того, нужно добавить ещё один блеклист - pbl.spamhaus.org.

Т.е. когда включаем режим проверки мыл, нужно проверять PTR и PBL. Для других режимов, не нужно. Боту отдаём мыла на проверку только в том случае если соблюдаются 2 условия: чистота по блеклистам + PBL и если есть PTR запись. Можно сделать эти проверки таким же образом, как реализована проверка на блеклисты. Т.е. новый бот стучит, проверяем по всем параметрам его, и на второй стук, если подходит, отдаём инфу.

Инфа от ботов приходит в следующем виде.

**Email !-! MX Server !-! Response from MX !-! Last response**

Если боту не удалось найти MX сервер то **MX Server = 0**, соответственно ответ будет таким **Email !-! 0 !-! 0 !-! 0**

Если боту не удалось соединиться с MX сервером в течение 30 сек, то отчёт бота такой **Email !-! MX Server !-! 0 !-! 0**

Нужно записать в базу эти параметры. Потом нужно обработать результаты, и тут начинается самое интересное.

Нужно обрабатывать конкретно «**Last response»,** обрабатывать мы его будем регуляркой с помощью крона. Причём придётся делать всё путём проб и ошибок.

«**Last response»** как правило содержит трёхзначный код, в соответствии с которым скрипт будет помечать мылы в базе.

Примеры «**Last response»** для понимания могут быть такими

550 5.4.1 Recipient address rejected: Access denied

250 2.1.5 Recipient Accepted

451 4.7.1 Greylisted - try again in 300 seconds

Скрипт будет вписывать 3 типа значения в поле Verification Result:

**Good** – если значение кода 250

**Bad** – если значение кода 550 или 450

**Unknown** – любые другие значения кодов

При этом возможен вариант когда значение кода 550 но письмо отклонено по разным причинам. Например

550 5.5.0 Your IP is blacklisted by FortiGuard. This email from IP has been rejected. The email message was detected as spam.

Нужно предусмотреть регулярные выражения для анализа ответа.

Допустим если «**Last response»** содержит слово Blacklist нужно помечать мыло как **Unknown.**

В панели нужно предусмотреть ввод подобных регулярных выражений при наличии которых помечаем как **Unknown.**