



Introduction to the MailProve Anti-Spam Blacklist

Written by: *Mr. Jeffrey Vong*
Date: *July 1st, 2005*



Table of Contents

INTRODUCTION..... 3

RATIONALE FOR CREATING MAILPROVE ANTI-SPAM BLACKLIST 3

 UNPLUG CONCEPT 3

 ISOLATE CONCEPT 4

 MAILPROVE’S TARGET..... 4

BLACKLIST RANGE 5

CENSORSHIP AND FREE SPEECH..... 5

ASIA SPECIFIC SPAM ISSUES 5

BLACKLIST REASONS..... 5

 DUE TO SPAM SOURCE 5

 DUE TO USE OF POOR MANAGED MAILING LISTS 5

 DUE TO SPAM RELAYING..... 5

 DUE TO OPEN RELAY 5

 DUE TO NON-VERIFY EMAIL REQUEST SERVICES 6

 DUE TO VIRUS SOURCE 6

LISTING PROCESS..... 6

DE-LISTING PROCESS 6

Introduction

The MailProve anti-spam blacklist was established in 2003 and is the most comprehensive, database of IP addresses that are known sources of poor managed email server which attack Asia Pacific. The MailProve anti-spam blacklist a carefully maintained list of IP addresses that have been shown to send trouble email.

The MailProve anti-spam blacklist Service allows for the creation of intentional network outages ("blackholes") for the purpose of limiting the transport of known-to-be-unwanted trouble email. Because it is a subscription system, the denied connectivity to trouble email server is only available for MailProve's customers.

For a complete anti-spam solution, we believed that it will require 2 levels of spam control. They are on network and content control level.

For content level control, there are email filters which check every email get into the email system but it does not help to stop the spam source. On the bright side, it control spam in very detail.

For network level control, there are blacklist which identify the spam sources and it provide information for the mail server to reject the mail from the spam source. It will alert the user and the email administrator to fix the spam problem on their email server.

Rationale for Creating MailProve Anti-Spam Blacklist

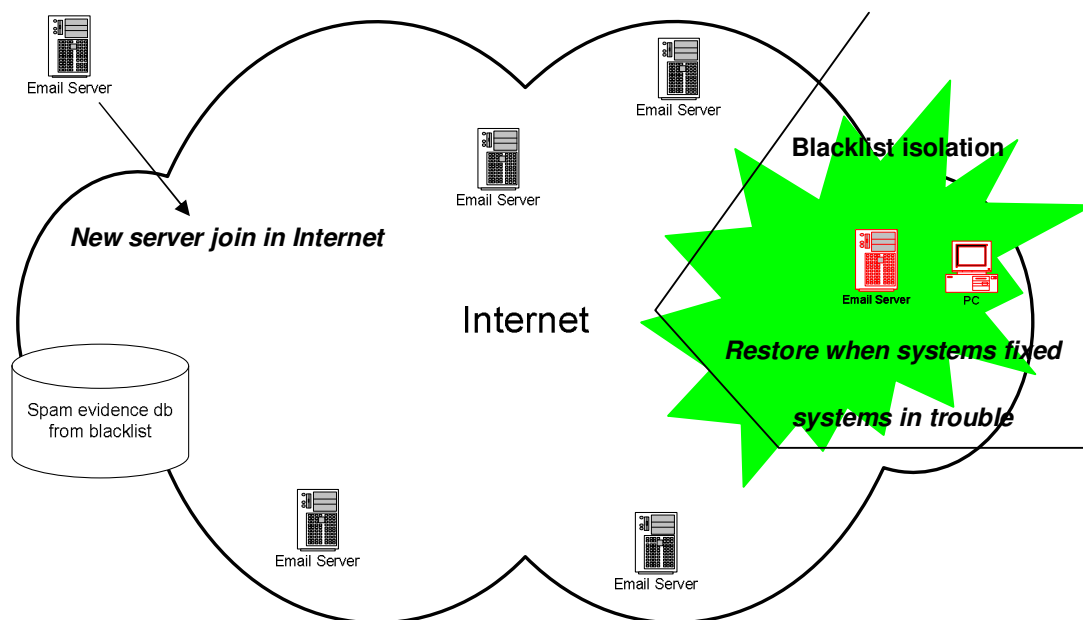
Unplug concept

For example, an electric appliance was out of order. The common practice is to remove the appliance from the power plug and get the problem fixed. After it is fixed, it can be plug into the power socket and use as normal.



Isolate concept

The email administrator may not be able to unplug a server on Internet which is out of order (sending spam to his server) but he can isolate that server on its own by using blacklist. The blacklist can also help him to force the email administrator of the spamming server to correct the spam problem. It is done by the users of the blacklisted email server told their email administrator that their email got rejected.



MailProve's Target

Email administrator is very concern of the spam they had received on their system because their user will complain to him. Without blacklist, they do not really care of the spam that was send from their server. Blacklist system will make sure the user of the sending server will complain to their email administrator that they can not send mail because of spam source from their email server.

MailProve anti-spam blacklist was targeted to build as an alert system to email administrator which is managing an email server that is in trouble. MailProve anti-spam blacklist can temporary isolate the mail servers in trouble until they get their problem fixed. MailProve operate will an effective listing and de-listing policy which make sure the email administrators get their out-bound spam problem fixed.

MailProve is also very focusing to the Asia specific spam problems as well as other problem related to email for example virus and phishing.

Blacklist Range

MailProve anti-spam blacklist identify spamming server is per IP basis. MailProve anti-spam blacklist only list the IP address that had an evidence support. Clean email servers from the same IP segments or same domain will not be affected.

Censorship and Free Speech

MailProve do not police the Internet, but rather offer a method to identify likely origins of spam. MailProve support free speech and no content censorship on the whole blacklist operation.

Asia Specific Spam Issues

MailProve anti-spam blacklist had define special logic to achieve a high detection rate of Asia specific spam. Although different locations in Asia use the same internal code for their contents, their local means, dialogs and cultures are totally different. Therefore MailProve had developed special library to address needs in different culture but same language issues.

Blacklist Reasons

In this section we describe some of the reasons an IP address may get listed on the MailProve anti-spam blacklist.

Due to Spam Source

Email server or email gateway which send spam up to pre-define volume.

Due to Use of Poor Managed Mailing Lists

Email server or email gateway which send to non-exist recipients or send to recipients which had request for un-subscribe from the mailing list.

Due to Spam Relaying

Email server or email gateway which relay email for their client even the content was spam or virus.

Due to Open Relay

Email server or email gateway which is open relay.



Due to Non-Verify email Request Services

Email server or email gateway which send email base on non-verify request on Internet.

Due to Virus Source

Email server or email gateway which send virus.

Listing Process

Any email server or email gateway which meets any condition of the above will be listed automatically.

De-listing Process

MailProve anti-spam blacklist support self service de-list request. The changes will be effective with 10 minutes from the request on <http://admin.mailrpove.net>.

There is also an auto de-list feature which is under the following schedule

Auto delist timer	Grace period (monitor only)	Communicative removal
24 hours (1 days)	24 hours (1 days)	0
48 hours (2 days)	48 hours (2 days)	1
96 hours (4 days)	96 hours (4 days)	2
192 hours (8 days)	192 hours (8 days)	3
384 hours (16 days)	384 hours (16 days)	4
n/a (call MailProve operator)	768 hours (32 days)	5

For example, without any additional spam detected, the blacklist IP address will be remove after 24 hours on 0 communicative removal records.

After the IP was removed from the first time, the IP will be under monitor for 24 hours (grace period). The grace period is not a blacklist period but any blacklist during this period will increase the communication removal counter by 1.

If there is no spam detect during the grace period, the communicative removal counter will reset to 0 and the blacklist history of that IP address will be removed.

For operator de-list service, MailProve operator will request for a reason why the spam problem was not resolved on the last 5 times of blacklist removal.