Spam Blocker Configuration Guide

This modification requires you to apply for 3rd party API keys in order to use its anti-spam resources from those third parties and enable it to function properly. These API keys are free of charge, however you are required to become a member on those 3rd party resource forums to acquire those API keys.

Please acquire API keys from the following forums:

Project Honeypot: https://www.projecthoneypot.org/

Akismet: https://akismet.com/signup/

Stop Forum Spam: http://www.stopforumspam.com/forum/

These API keys will allow this modification to use those 3rd party databases to filter users IP and email addresses during the registration process and will also allow topic/post filtering. You must enter the acquired API keys in the Spam Blocker configuration menu. Only use one API key from each source for every forum you install this modification onto. Do not use the same API key(s) on multiple forums or those 3rd parties may ban those keys.

All 3rd party anti-spam resources will use the 3 month (90 day) exemption if opted. Honeypot has more specific configuration including threat score and visitor types to allow. This modification will ignore threat scores that are below (not equal to) the integer that is entered for that text input. The visitor types input will allow a single input or multiple inputs (separated by commas) and will ignore those types if it encounters them from Honeypot's database. Both of these Honeypot inputs require integer values between 0 and 255.

Honeypot charts are shown on page 2 of this guide for configuring its threat score and visitor type values.

All of this modification's templates have help text that is available by selecting the various question mark links. With the main configuration page each option has its own explanation and the other templates have less options therefore one link is provided for each that gives detailed information regarding their functions and usage.

Any IP's added to the whitelist will be ignored at the time of registration and will not be subject to filtering through the various anti-spam resources.

IP's and/or email addresses flagged by the 3rd party anti-spam resources as spam will be automatically added to both this modification's blacklist and your forum's ban list. Deleting those entries from either list will cross check each others database tables and your member list to properly delete any related data from your database. This is to ensure no deleted ban entitiy will become a member of your forum. The only way to keep the member id in your database while deleting an entity from your ban list and blacklist is to use this modification's blacklist template and uncheck the subjoined member id checkbox.

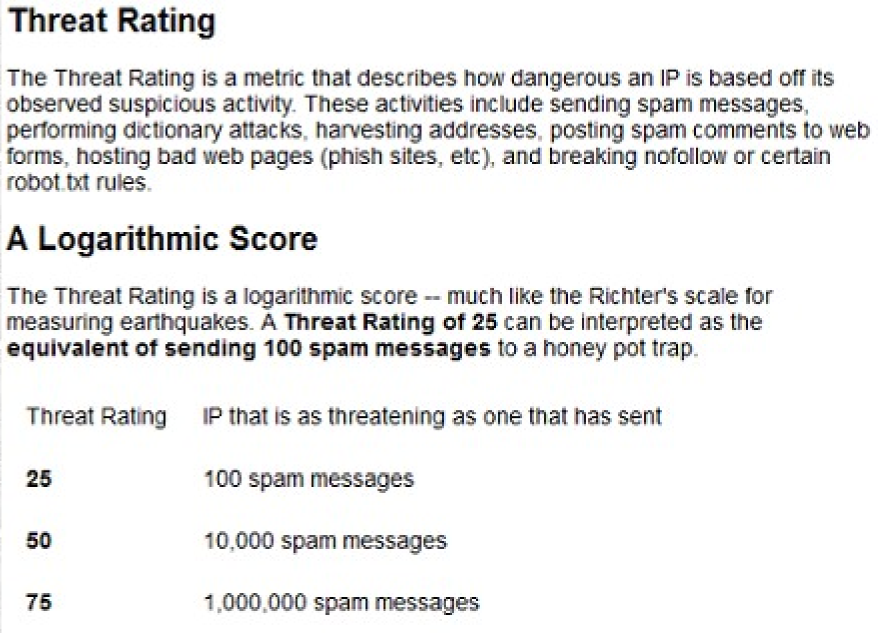
The blacklist template will allow you to view the banned/blacklisted entities that this modification has added to your database in an organized fashion. It provides two forms of pagination to allow easy viewing of lengthy lists which will accumulate over time. It is advised to manage your banned entities added by this modification through that template.

This modification also provides a template for manually checking IP's and/or email addresses through the anti-spam databases. Please note that you must have those anti-spam resources enabled in the configuration menu to utilize their database information.

Various maintenance functions are available in the configuration menu although this modification should function properly without their use, circumstances may require them. This modification will check the database every three to six hours to delete any expired bans and their associated member id's (maximum 500 queries per 3 hrs).

You are advised to set an expiration on banned entities due to dynamic IP assignment by various ISP's.
This means that Ipv4 addresses can be reassigned to legitimate users after a period of time.

Threat Score Value Guide



Threat Rating

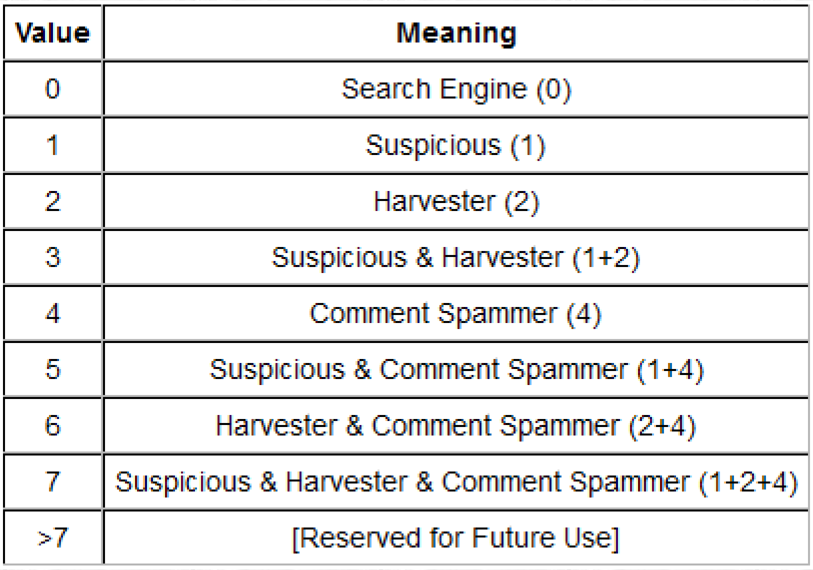
The Threat Rating is a metric that describes how dangerous an IP is based off its observed suspicious activity. These activities include sending spam messages, performing dictionary attacks, harvesting addresses, posting spam comments to web forms, hosting bad web pages (phish sites, etc), and breaking nofollow or certain robot.txt rules.

A Logarithmic Score

The Threat Rating is a logarithmic score -- much like the Richter's scale for measuring earthquakes. A **Threat Rating of 25** can be interpreted as the **equivalent of sending 100 spam messages** to a honey pot trap.

Threat Rating	IP that is as threatening as one that has sent
25	100 spam messages
50	10,000 spam messages
75	1,000,000 spam messages

Visitor Types Value Guide



Value	Meaning
0	Search Engine (0)
1	Suspicious (1)
2	Harvester (2)
3	Suspicious & Harvester (1+2)
4	Comment Spammer (4)
5	Suspicious & Comment Spammer (1+4)
6	Harvester & Comment Spammer (2+4)
7	Suspicious & Harvester & Comment Spammer (1+2+4)
>7	[Reserved for Future Use]

Recommended minimal requirements:
Server: PHP 5.2+ with libxml, cURL, socket connections & DOM enabled ~ HTML5+ ~ MYSQL 5.0+ using MyISAM or InnoDB engine
Browser Add-Ons (for admin): Adobe Flashplayer 11.5+, JRE 7.10+
Forum Software: SMF Version: 2.0.4+

Annotation: Do not edit the note text from entries added to your ban list from Spam Blocker. They are used as a reference for when this modification omits blacklist/ban list entities.

Developed for SMF forums c/o Underdog @ webdevelop.comli.com