EsAntispam 2.0

Antispam and hackbots protection

Copyright

Publication date and software version

Published August 2020. Based on EsAntispam 2.0

Contents

Preface

What is this module for?

This module primary aim is to protect all PrestaShop based shop from spammer. While this goal was first, over time this module has evolved and provide either some nice protection against hacking attempts.

Minimum requirements for using the module

You need PrestaShop version 1.6+, with PHP 5.6+ and openssl PHP extension. (most PHP has it by default). The module is compatible up to PHP 7.4 to date.

How to get EsAntispam

Versions of EsAntispam are excluvely available at Enter-Solutions' shop, and can be order at https://store.enter-solutions.com

Frequently asked questions

May I distribute EsAntispam to anyone? May I sell it?
No. This module is licensed to a single shop.

How many computers may I install it on?
Only one shop, either single or multi-shop.

How can I get a license for my prestage environment?
This module dealing with internet in the wild, there is no need for it to be operative inside your pre-stage env. Since the license will not match your preprod shop's domain it will simply do nothing.

But I absolutely need a license for my preprod !
Contact-us we will assess your need and issue a special license for the pre-stage.

I have lost my license, how do I get it back?
Logon to your Enter-Solutions' user account. The license can be generated for the Order History page.

Chapter 1 - Installation

Module installation

To proceed with installation, we recommend using the PrestaShop installation method from the back-office.

First download on your computer the module from Enter-Solutions' Order History page within customer profile.

One the download completed, connect to your shop's back-office with an employee account having SuperAdmin rights.

Proceed as follow:

1. Select menu "Modules and Services
2. Click sub-menu "Modules and Services"
3. Click button "Add a new module"
4. Use button "Choose a file" and select the module you downloaded from your computer
5. Click "Upload this module"

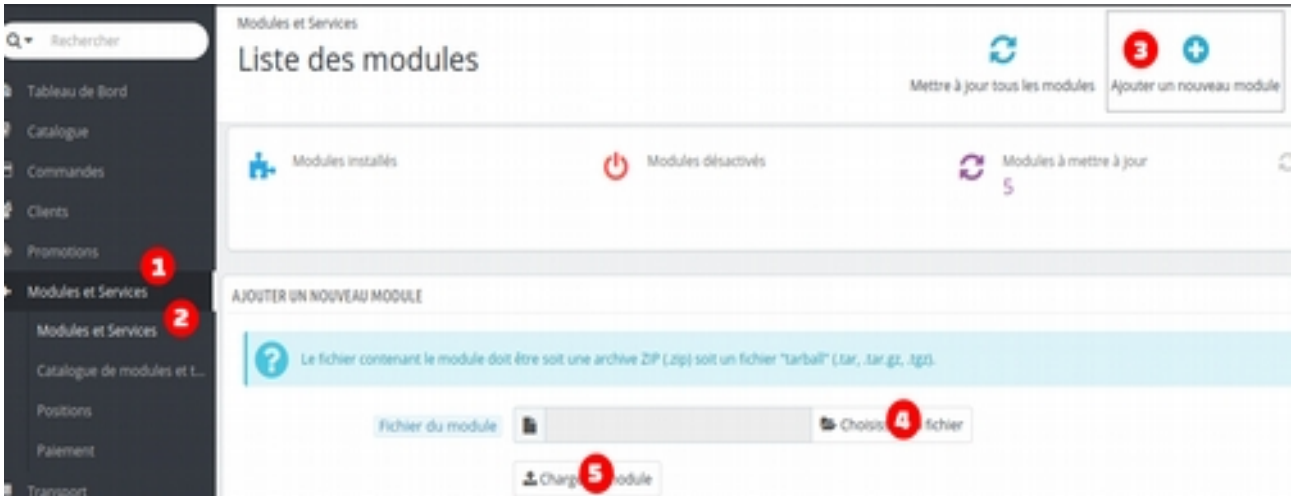

Figure 1: Recommended installation steps

If the module does not automatically install, proceed by clicking the button "Install".

Note

Should a problem occurs after installation, See Chapter 3, Troubleshooting, for more information.

License installation

This module requires a license to operate. This license can be obtained from Enter-Solutions' Order History page within customer profile. It can also be obtained by following the link that appears in the module's configuration page.

Download and save the license file in a similar manner you did for module file. Once downloaded the installation is similar to installing the module. Choose "add a new module" and proceed accordingly.

Caution

Do not tamper with the license file. It uses asymmetric key encryption mechanism and is therefore not human readable.

Tip

Should you loose or corrupt your license file, it could be re-issued any time from your Enter-Solutions' Order History page.

Configuration

This module consists of several separated components – called plugins - that help avoid various spams whether bot or human bases. Each plugins can be activated/configured separately. For more information regarding each plugin refer to Chapter 2, Plugins.

CRON

Either plugins or module in itself needs some daily action to be executed to cleanup and ??.

Those tasks are listed at the bottom of the module configuration page. You may need to setup those tasks to be executed on a daily basis should you want the module to behave as designed.

Chapter 2 - Plugins

KOOK protection

The purpose of this plugin is to actively detect programmatic form submission. This plugins is self contained and requires no configuration.

Upon such mis-behaviour be detected, the form submission is immediately intercepted and does not enter the PrestaShop framework.

Email filtering

Hackers, or spambots regularly use disposable email address. This protect their identify and makes it difficult to track them later on. This module uses well known list of such disposable email domain and prevent account registration or newsletter subscription using those known email domains.

On top of the proposed list of known email domain, you can define your own list of source including your own personal one by having a file available over the web. Should any use such email domain, it is detected and returned as an invalid email address.

Figure 2: Email filter configuration

Disposal list

Sources of list of known disposal email domain. The list format is pretty versatile to accommodate with various sources. You can as well define your own list making it reachable over the web. Entries in the list (one per line) follow the following format:

priority	***format***	***action***
1	<regex>	domain is always accepted
2	-<regex>	Domain is banned

Tip

Slash (/) is not a special character and need not to be escaped.
Negation (hyphen) always take precedence.

Caution

This plugin need its counter-part CRON job to set to operate properly

TOR filtering

Often hackers or spambots hide themselves behind connection issued from the TOR network. This plugins uses live updated list of TOR exit points to filter, by IP such connection attempts.

On top of the regular TOR exit list, you can use any other list of node by having a file available over the web.

Any connection from an IP address within the lists are immediately block. No further processing enters the PrestaShop framework.

Figure 3: TOR configuration

TOR list

Publicly available list of TOR exit nodes. This is the official up-to-date (6 hours) list of nodes published by the Onion project. Should you know a more accurate list, add a source url (one per line).

Caution

This plugin need its counter-part CRON job to set to operate properly

AbuseIPDB

AbuseIPDB is an online service that provide the most accurate list of known abusing IP. It can be compromised system that are ordinarily harmless, or permanent hackbot/spambot abuser.

Because AbuseIPDB has a free although limited plan, it can be a good choice to integrated such list of corrupted IP to be excluded to interfere with the shop.

You'll need to subscribe to an IPDB subscription plan and obtain an API key to activate this plugins.

Any connection from an IP address within the lists are immediately block. No further processing enters the PrestaShop framework.

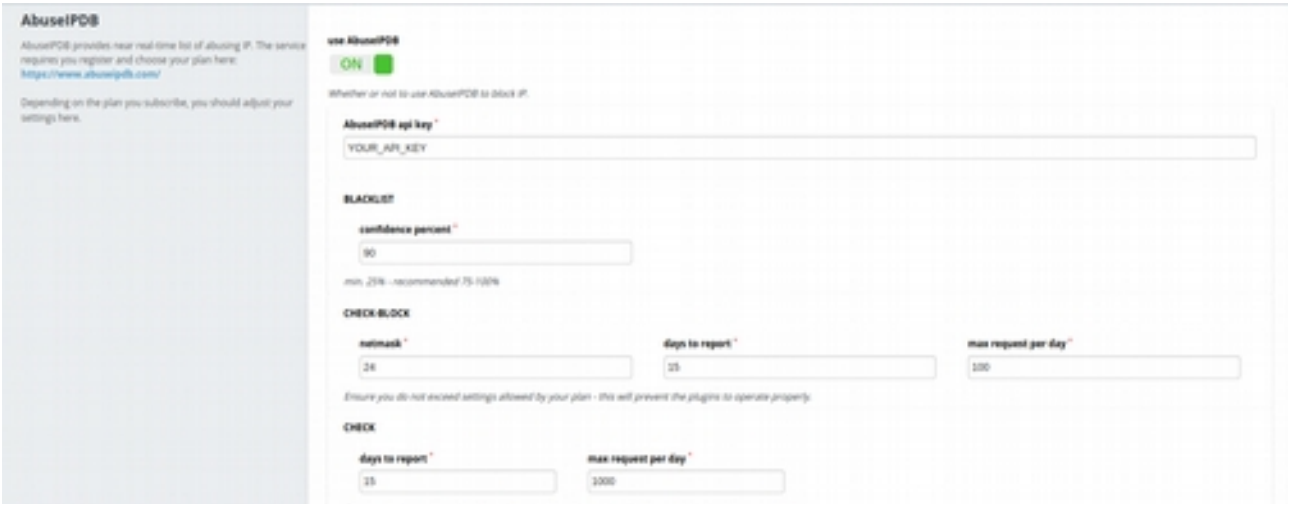

Figure 4: IPDB filter settings

AbuseIPDB API key

The API key related to your IPDB subscription plan

BLACKLIST / confidence percent

From which percent of confidence would you like to block the corresponding IPs

CHECK-BLOCK

Settings related to throttling calls to this API. The default values (24/15/100) matches the parameters needed for the free subscription plan.

CHECK

Settings related to throttling calls to this API. The default values (15/1000) matches the parameters needed for the free subscription plan.

Caution

This plugin need its counter-part CRON job to set to operate properly

Google recaptcha

A nice addition to prevent spammer is using the Google recaptcha engine. This plugins provide an easy integration of Google recaptcha v2.

The choice from the plugin is to makes this recaptcha visible.

Figure 5: Google recaptcha configuration

Site key

The site key provided by Google. Be sure when you set your key to include all top-level domain of your shop.

Secret key

The secret key as provided by Google.

Waste time

Should the Google recaptcha verification fails (after submission), we enforce some random wait time. This slow brute-force attacks and makes-it unpredictable programmaticaly.

Legal snippet

Add a snipped in the page footer “powered by Google”.

Tip

The template fully can be customized in themes/<your-theme>/modules/esantispam/legal.tpl

Hackbots filtering

Hackbots are prone to use well known pattern to try penetrating shops. While some pattern may not be successful they are recognizable, hence trigger an alert that such visitor intend criminal activities. This plugin provide a mechanism to detect such unsuccessful attempt and decide to ban the offending IP.

Figure 6: Hackbots filter configuration

Grace period

Upon detection the hackbot's IP address is stored for that amount of time in seconds.

Pattern list

Specify the pattern that trigger a positive detection (one per line). Patterns are regex. Slash (/) is not a special character and need not to be escaped.

Tip

Searching thru the "Page not found" statistics page can help you identify new pattern for inclusion.

Caution

This plugin need its counter-part CRON job to set to operate properly

Upload filtering

Should hackers find a security loophole, they will use it to upload various content. It can be exploit flag, but more certainly a series of tools that are even easier backdoor. By actively filtering uploaded content you can prevent such exploit to lead to even higher infection.

The filtering is done at early stage avoiding any undesirable content to reach the PrestaShop framework.

Figure 7: Upload filter configuration

Log all upload

When activated, all upload hitting the public portion of the shop are logged. Whether filtered or not. Useful to investigate tampered files should a penetration occurred.

Remove path data

When a file is uploaded, the browser (client) can propose a destination filename. This option filters out any path from this proposed name. Do such, prevent any file to be send to different location than expected.

Block file having such extensions

A list of file extension that SHOULD NOT be accepted (one per line)

Block non image file

Uploaded file are sensed to ensure they are only images. This use magic database.

Magic database

Enter the path of your own database should you want to use it in place of PHP internal's one

internal plugin

The internal plugin is always active it deserves three purposes. Implement a mechanism to by-pass filtering for some predefined proxies. It ists all the various CRONs related to different modules. Last it implement a mechanism to perform log cleanup and rotation.

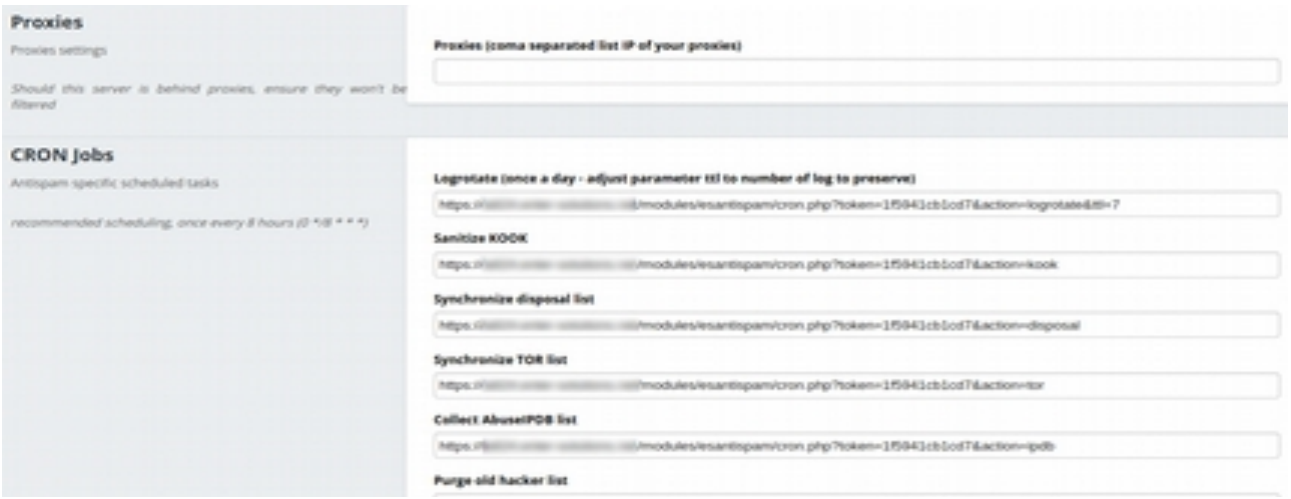

Figure 8: internal plugin

Chapter 3 - Troubleshooting

White Screen Of Death

Various situation can cause White-Screen-Of-Death (WSOD). Here is a step thru to address the issue.

1. If the WSOD only affects the Module's page, try clearing the cache in menu Advanced Parameters > Performances, click on the icon "Clear the cache" on upper right corner of the screen.
2. If you are on version 1.7+, try clearing the cache manually via FTP. Delete folders "var/cache/prod" and "var/cache/dev" from your PrestaShop's installation
3. Activate the debug mode by editing the file config/defines.inc.php, changing the line
   define('_PS_MODE_DEV_',false);
   by
   define('_PS_MODE_DEV_',true);
   Be sure to collect all information displayed after that point.
4. Using FTP, rename the folder "esantispam" in _esantispam.
5. Contact-us with the information you captured at step 3, desactivate the debug mode by reversing step 3 (I.e: settings back to false.

Customer reports false positive

If you encounter a situation where your customer cannot operate your shop normally, try one by one to disable plugins.

The plugin KOOK is using some aggressive technology to detect bots. It should be your first candidate.

Some users browse the web via the TOR network. If you feel comfortable allowing such network, disable TOR filtering.

Some customer may be infected by malware and therefore their PC is indeed part of an active hackbot network, check https://www.abuseipdb.com/ or https://www.badips.com/get/info/<customer-ip> that your customer's IP is not listed here. To help your customer report his own IP, ask him to browse this page: https://whatismyipaddress.com/

Consult the module log.

Read module specific log

Once the module detect some specific situation it block it and log reason to a log file modules/esantispam/logs/`forensic.log`.

If you have activated the always log upload on Upload filter plugin, the dedicated log is modules/esantispam/logs/`uploads.log.`