EsAntispam 2.0

Protection antispam et hackbots

Copyright

Date de publication et version du logiciel

Publié en août 2020. Basé sur EsAntispam 2.0

Contenu

Préface

A quoi sert ce module?

L'objectif principal de ce module est de protéger toutes les boutiques basées sur PrestaShop contre les spammeurs. Alors que cet objectif était le premier, au fil du temps, ce module a évolué et offre une bonne protection contre les tentatives de piratage.

Exigences minimales pour l'utilisation du module

Vous avez besoin de la version 1.6+ de PrestaShop, avec PHP 5.6+ et l'extension PHP openssl. (la plupart des PHP l'ont par défaut). Le module est compatible jusqu'à PHP 7.4 à ce jour.

Comment obtenir EsAntispam

Les versions d'EsAntispam sont disponibles en exclusivité dans la boutique d'Enter-Solutions et peuvent être commandées sur https://store.enter-solutions.com

Questions fréquemment posées

Puis-je distribuer EsAntispam à n'importe qui? Puis-je le vendre?
Non. Ce module est concédé sous licence à un seul magasin.

Sur combien d'ordinateurs puis-je l'installer?
Un seul magasin, unique ou multi-boutique.

Comment puis-je obtenir une licence pour mon environnement de pré-production?
Ce module protégeant des accès internet, il n'est pas nécessaire qu'il soit opérationnel dans votre environnement pré-production. Étant donné que la licence ne correspondra pas au domaine de votre boutique de pré-production, il ne fera tout simplement rien.

Mais j'ai absolument besoin d'une licence pour ma pré-production!
Contactez-nous, nous évaluerons votre besoin et délivrerons une licence spéciale pour la pré-production.

J'ai perdu ma licence, comment la récupérer?
Connectez-vous à votre compte utilisateur Enter-Solutions. La licence peut être générée depuis la page Historique des commandes.

Chapter 1 - Installation

Installation du module

Pour procéder à l'installation, nous vous recommandons d'utiliser la méthode d'installation PrestaShop depuis le back-office.

Téléchargez d'abord sur votre ordinateur le module à partir de la page Historique des commandes d'Enter-Solutions dans le profil client.

Une fois le téléchargement terminé, connectez-vous au back-office de votre boutique avec un compte employé disposant des droits SuperAdmin.

Procédez comme suit:

1. Sélectionnez le menu «Modules et services
2. Cliquez sur le sous-menu "Modules et services"
3. Cliquez sur le bouton "Ajouter un nouveau module"
4. Utilisez le bouton «Choisir un fichier» et sélectionnez le module que vous avez téléchargé depuis votre ordinateur
5. Cliquez sur "Télécharger ce module"

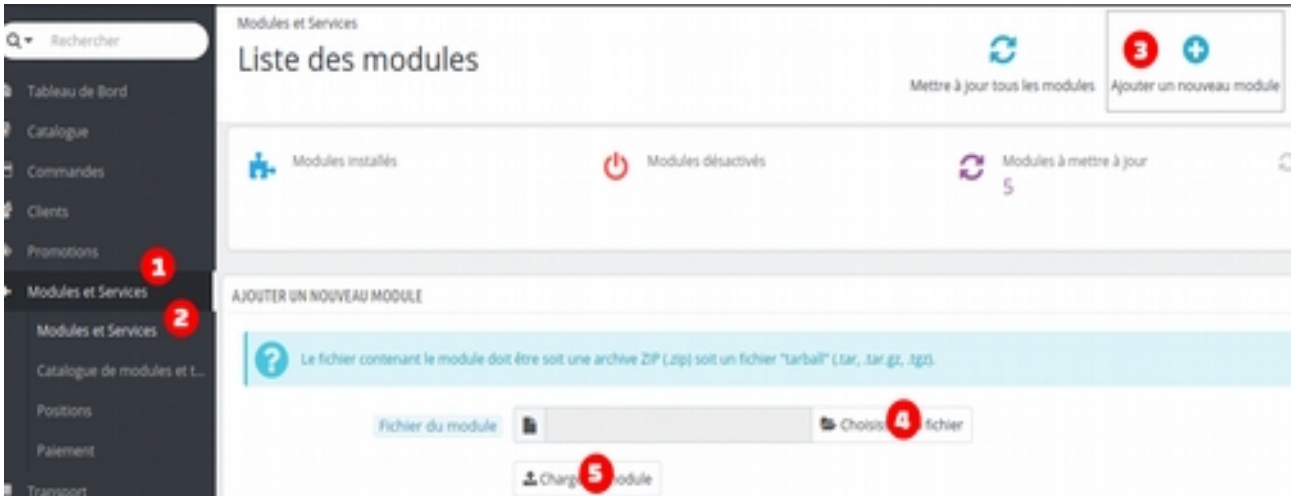

Figure 1: Etapes d'installation

Si le module ne s'installe pas automatiquement, continuez en cliquant sur le bouton «Installer».

Note

Si un problème survient après l'installation, reportez-vous au chapitre 3, Dépannage, pour plus d'informations.

Installation de la licence

Ce module nécessite une licence pour fonctionner. Cette licence peut être obtenue à partir de la page Historique des commandes d'Enter-Solutions dans le profil client. Elle peut également être obtenue en suivant le lien qui apparaît dans la page de configuration du module.

Téléchargez et enregistrez le fichier de licence de la même manière que vous l'avez fait pour le fichier de module. Une fois téléchargée, l'installation est similaire à l'installation d'un module. Choisissez «ajouter un nouveau module» et procédez en conséquence.

Attention

Ne modifiez pas le fichier de licence. Il utilise un mécanisme de cryptage à clé asymétrique et n'est donc pas lisible par par un humain.

Astuce

Si vous perdez ou corrompez votre fichier de licence, il peut être réémis à tout moment à partir de la page Historique des commandes d'Enter-Solutions.

Configuration

Le module se compose de plusieurs composants séparés - appelés plugins - qui permettent d'éviter divers spams, qu'ils soient d'origine humaine ou robot. Chaque plug-in peut être activé / configuré séparément. Pour plus d'informations sur chaque plugin, reportez-vous au Chapitre 2, Plugins.

CRON

Soit les plugins, soit le module en lui-même nécessite une action quotidienne des nettoyages et un fonctionnement optimal.

Ces tâches sont répertoriées au bas de la page de configuration du module. Vous devrez peut-être configurer ces tâches pour qu'elles soient exécutées quotidiennement si vous souhaitez que le module se comporte comme prévu.

Chapitre 2 - Plugins

KOOK protection

Le but de ce plugin est de détecter activement la soumission de formulaires programmatiques. Ce plugin est autonomes et ne nécessitent aucune configuration.

Lorsqu'un tel comportement erroné est détecté, la soumission du formulaire est immédiatement interceptée et n'entre pas dans le cœur de PrestaShop.

Filtrage des e-mails

Les pirates informatiques ou les spambots utilisent régulièrement une adresse e-mail jetable. Cela protège leur identité et rend difficile leur suivi par la suite. Ce module utilise une liste bien connue de ces domaines de messagerie jetables et empêche l'enregistrement de compte ou l'abonnement à la newsletter qui utiliseraient ceci.

Figure 2: Email filter configuration

En plus de la liste proposée des domaines e-mails connus, vous pouvez définir votre d'autres sources, y compris la vôtre, en ayant un fichier disponible sur le Web. Si un visiteur utilise un tel domaine de messagerie, il est détecté et bloqué comme ayant une adresse e-mail non valide.

Liste des domaines jetable

Sources de la liste du domaine d'e-mail jetable connu. Le format de liste est assez polyvalent pour s'adapter à diverses sources. Vous pouvez également définir votre propre liste pour la rendre accessible sur le Web. Les entrées de la liste (une par ligne) suivent le format suivant:

priorité	***format***	***action***
1	-<regex>	le domaine est toujours accepté
2	<regex>	Domaine est interdit

Astuce

La barre oblique (/) n'est pas un caractère spécial et n'a pas besoin d'être échappée. La négation (trait d'union) a toujours la priorité.

Attention

Ce plugin a besoin d'une tâche CRON associée pour fonctionner correctement

Filtrage TOR

Souvent, les hackers ou les spambots se cachent derrière une connexion issue du réseau TOR. Ce plug-in utilise une liste mise à jour en direct des points de sortie TOR pour filtrer, par IP, de telles tentatives de connexion.

En plus de la liste de sortie TOR classique, vous pouvez utiliser n'importe quelle autre liste de nœuds en ayant un fichier disponible sur le Web.

Toute connexion à partir d'une adresse IP reconnues est immédiatement bloquée. Aucun autre traitement n'entre dans le framework PrestaShop.

Figure 3: TOR configuration

Liste TOR

Liste publique des nœuds de sortie TOR. Il s'agit de la liste officielle à jour (6 heures) des nœuds publiée par le projet Onion. Si vous connaissez une liste plus précise, ajoutez une URL source (une par ligne).

Attention

Ce plugin a besoin d'une tâche CRON associée pour fonctionner correctement

AbuseIPDB

AbuseIPDB est un service en ligne qui fournit la liste la plus précise des IP ayant été marquées comme abusives. Il peut s'agir d'un système compromis qui est normalement inoffensif ou d'un hackbot / spambot abusif permanent.

Parce qu'AbuseIPDB a un plan gratuit bien que limité, il peut être un bon choix d'intégrer une telle liste d'adresses IP corrompues à exclure de la boutique.

Vous devrez vous abonner à un plan d'abonnement IPDB et obtenir une clé API pour activer ce plugin.

Toute connexion à partir d'une adresse IP dans les listes est immédiatement bloquée. Aucun autre traitement n'entre dans le framework PrestaShop.

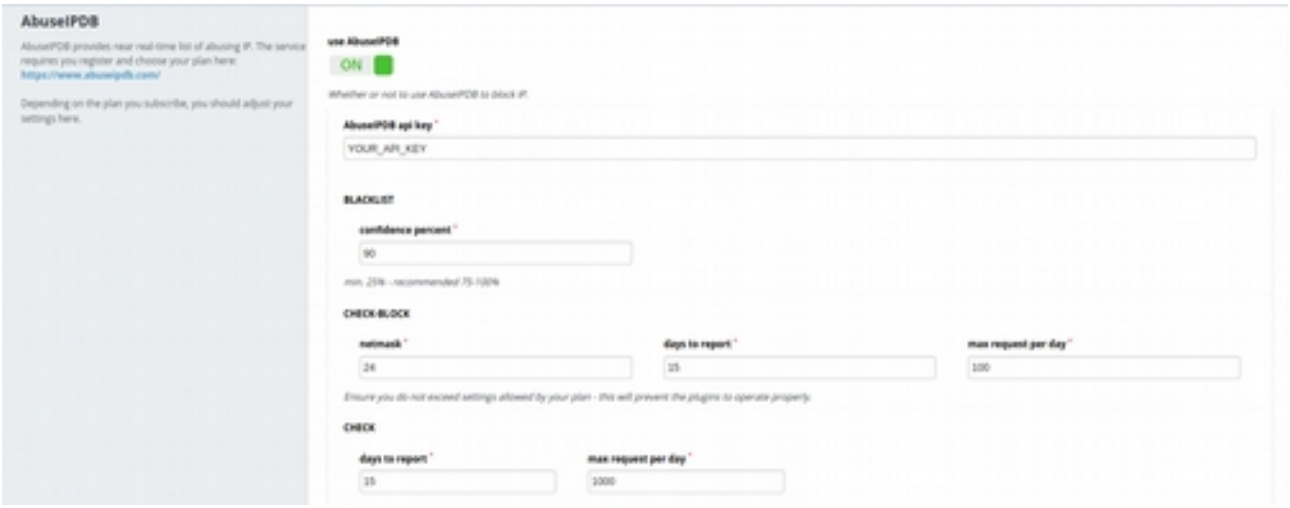

Figure 4: IPDB filter settings

Clé API AbuseIPDB

La clé API liée à votre plan d'abonnement IPDB

BLACKLIST / pourcentage de confiance

À partir de quel pourcentage de confiance souhaitez-vous bloquer les adresses IP correspondantes

CHECK-BLOCK

Paramètres liés à la limitation des appels à cette API. Les valeurs par défaut (24/15/100) correspondent aux paramètres nécessaires pour le plan d'abonnement gratuit.

CHECK

Paramètres liés à la limitation des appels à cette API. Les valeurs par défaut (15/1000) correspondent aux paramètres nécessaires pour le plan d'abonnement gratuit.

Attention

Ce plugin a besoin d'une tâche CRON associée pour fonctionner correctement

Google recaptcha

Un ajout intéressant pour empêcher les spammeurs est d'utiliser le moteur de recaptcha de Google. Ce plugin fournit une intégration facile de Google recaptcha v2.

Le choix du plugin est de rendre ce recaptcha visible.

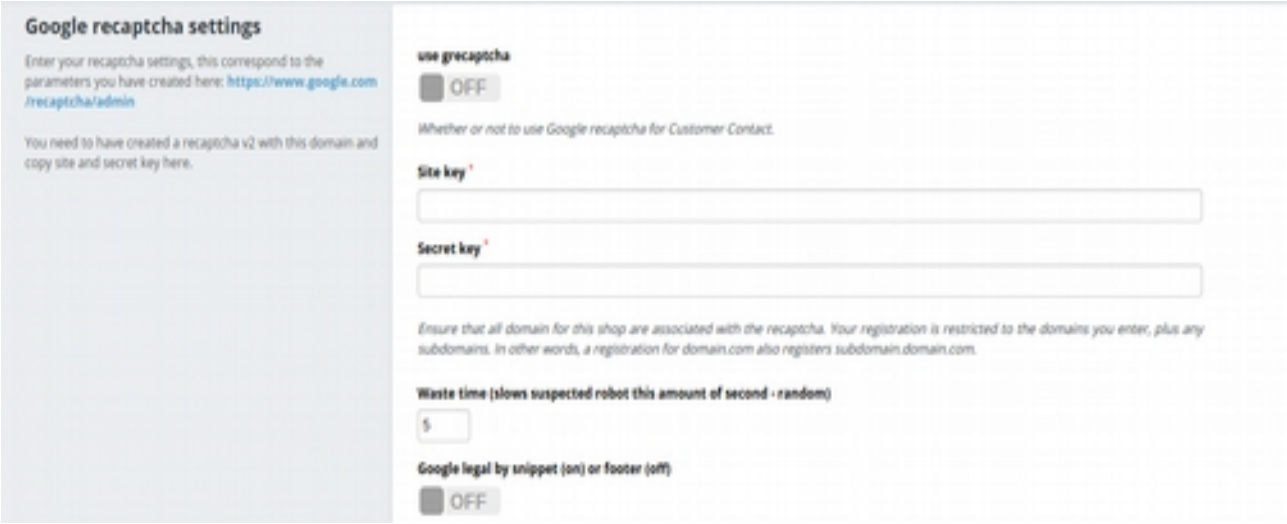

Figure 5: Google recaptcha configuration

Site key

La clé de site fournie par Google. Lorsque vous définissez votre clé, assurez-vous d'inclure tous les domaines de premier niveau de votre boutique.

Secret key

La clé secrète fournie par Google.

Retard

Si la vérification de Google recaptcha échoue (après la soumission), nous appliquons un temps d'attente aléatoire. Ceci ralenti les attaques par force brute et rend la programmation imprévisible.

Vignette legale

Ajoutez un extrait dans le pied de page "powered by Google".

Astuce

Le modèle peut être entièrement personnalisé dans les thèmes/<your-theme> /modules/esantispam/legal.tpl

Filtrage des hackbots

Les hackbots ont tendance à utiliser des modèles bien connus pour essayer de pénétrer les boutiques. Bien que certaines tentatives puissent ne pas réussir, ils sont reconnaissables, ce qui déclenche une alerte indiquant que ce visiteur a l'intention d'activités criminelles. Ce plugin fournit un mécanisme pour détecter une telle tentative infructueuse et décider d'interdire l'IP incriminée.

Figure 6: Hackbots filter configuration

Période de grâce

Lors de la détection, l'adresse IP du hackbot est stockée et bloquée pendant cette durée en secondes.

Liste des motifs

Spécifiez le motif qui déclenche une détection positive (une par ligne). Les motifs sont des regex. La barre oblique (/) n'est pas un caractère spécial et n'a pas besoin d'être échappée.

Pointe

La recherche sur la page de statistiques «Page non trouvée» peut vous aider à identifier un nouveau motif à inclure.

Attention

Ce plugin a besoin d'une tâche CRON associée pour fonctionner correctement

Filtrage des téléversements

Si les pirates trouvent une faille de sécurité, ils l'utiliseront pour télécharger divers contenus. Il peut s'agir d'un drapeau d'exploit, mais plus certainement d'une série d'outils qui contiennent encore plus de portes dérobées. En filtrant activement le contenu téléchargé, vous pouvez empêcher qu'un tel exploit ne conduise à une infection encore plus élevée.

Le filtrage se fait à un stade précoce en évitant tout contenu indésirable d'atteindre le framework PrestaShop.

Figure 7: Upload filter configuration

Enregistrer tous les téléversements

Lorsqu'il est activé, tous les téléversements touchant la partie publique de la boutique sont enregistrés. Qu'ils soient filtrés ou non. Utile pour enquêter sur les fichiers falsifiés en cas de pénétration.

Supprimer les données de chemin

Lorsqu'un fichier est téléversé, le navigateur (client) peut proposer un nom de fichier de destination. Cette option filtre tout chemin de ce nom proposé. Ceci permet d'empêcher au fichier d'être envoyé à un emplacement différent de celui prévu.

Bloquer le fichier ayant de telles extensions

Une liste d'extensions de fichiers qui NE DEVRAIT PAS être acceptées (une par ligne)

Bloquer les fichiers non image

Les fichiers téléchargés sont inspectés pour s'assurer qu'il ne s'agit que d'images. On utilise pour cela la base de données magique.

Base de données magique

Entrez le chemin de votre propre base magique si vous souhaitez l'utiliser à la place de celle interne de PHP

plugin interne

Le plugin interne est toujours actif il désert trois objectifs. Implémenter un mécanisme pour contourner le filtrage pour certains proxys prédéfinis. Il regroupe tous les différents CRON liés aux différents plugins. Enfin, il implémente un mécanisme pour effectuer le nettoyage et la rotation des journaux.

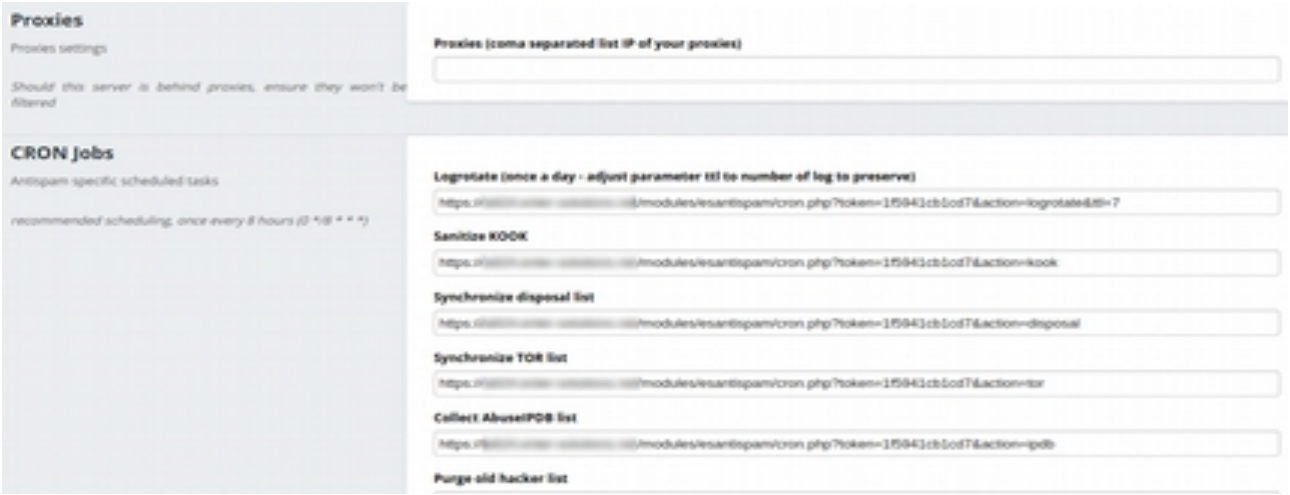

Figure 8: internal plugin

Chapitre 3 - Dépannage

Écran blanc de la mort

Diverses situations peuvent provoquer un écran blanc de la mort (WSOD). Voici les étapes à suivre pour résoudre ce problème.

1. Si le WSOD n'affecte que la page du module, essayez de vider le cache dans le menu Paramètres avancés> Performances, cliquez sur l'icône «Vider le cache» dans le coin supérieur droit de l'écran.
2. Si vous utilisez la version 1.7+, essayez de vider le cache manuellement via FTP. Supprimez les dossiers «var/cache/prod» et «var/cache/dev» de l'installation de votre PrestaShop
3. Activez le mode débogage en éditant le fichier config / define.inc.php, en changeant la ligne define («_ PS_MODE_DEV _», false); par define («_ PS_MODE_DEV _», true); Assurez-vous de collecter toutes les informations affichées après ce point.
4. À l'aide de FTP, renommez le dossier «esantispam» dans _esantispam.
5. Contactez-nous avec les informations que vous avez capturées à l'étape 3, désactivez le mode de débogage en inversant l'étape 3 (c'est-à-dire: remettre la valeur false).

Un client signale un faux positif

Si vous rencontrez une situation dans laquelle votre client ne peut pas faire fonctionner votre boutique normalement, essayez un par un pour de désactiver les plugins.

Le plugin KOOK utilise une technologie agressive pour détecter les bots. Celui-ci devrait être votre premier candidat.

Certains utilisateurs naviguent sur le Web via le réseau TOR. Si vous vous sentez à l'aise d'autoriser un tel réseau, désactivez le filtrage TOR.

Certains clients peuvent être infectés par des logiciels malveillants et donc leur PC fait effectivement partie d'un réseau de hackbot actif, consultez https://www.abuseipdb.com/ ou https://www.badips.com/get/info/<customer-ip > que l'adresse IP de votre client n'est pas répertoriée ici. Pour aider votre client à signaler sa propre adresse IP, demandez-lui de parcourir cette page: https://whatismyipaddress.com/

Consultez le journal du module.

Lire le journal spécifique au module

Une fois que le module a détecté une situation spécifique, il la bloque et enregistre la raison dans un fichier journal modules/esantispam/logs/`forensic.log`.

Si vous avez activé le téléchargement toujours du journal sur le plug-in de filtrage Upload, le journal dédié est modules/esantispam/logs/`uploads.log`.