Bloquer les attaques de type brute-force avec un fichier htaccess

Depuis maintenant plusieurs mois, des attaques de type “brute force” à grande échelle contre les installations WordPress, provenant d'une grande quantité d'adresses IP compromises réparties à travers le monde, a augmenté considérablement.

La technique que nous utiliserons pour bloquer les attaques aura pour effet de renvoyer vers un site (google.ca dans notre exemple) tous les utilisateurs dont l'accès est interdit aux fichiers wp-login.php, xmlrpc.php et au dossier wp-admin

L'accès à ces fichiers sera permise seulement aux utilisateurs dont l'adresse IP sera inscrite dans le fichier .htaccess à la racine de votre installation Wordpress.

Installation

Vous devez ajouter le contenu suivant complètement dans le haut dans le fichier .htaccess à la racine de votre installation Wordpress (avant # BEGIN WordPress).

ex: /home/NOM D'UTILISATEUR/domain/MON-DOMAINE.XXX/public_html/.htaccess

```
RewriteEngine on
RewriteCond %{REQUEST_URI} ^(.*)?wp-login\.php(.*)$ [OR]
RewriteCond %{REQUEST_URI} ^(.*)?xmlrpc\.php(.*)$ [OR]
RewriteCond %{REQUEST_URI} ^(.*)?wp-admin$
RewriteCond %{REMOTE_ADDR} !^123\.123\.123\.121$
RewriteRule ^(.*)$ http://www.google.ca [L,R=301]
```

Informations

Dans notre exemple, seulement l'adresse IP 123.123.123.121 peut voir/rejoindre les fichiers wp-login.php, xmlrpc.php et le dossier wp-admin

Tous les autres utilisateurs (avec d'autres adresses IP) ne seront pas en mesure de voir ces fichiers et seront renvoyés vers google.ca

IMPORTANT: Il est important de ne pas rediriger les attaques ou les utilisateurs n'ayant pas droit d'accès à ces fichiers sur un site hébergé sur le même serveur que le site que vous souhaitez protéger. Si les utilisateurs sont renvoyés sur un site hébergé sur le même serveur, cela aura pour effet d'augmenter considérablement la charge du serveur d'hébergement lors de la période d'attaque par brute-force. C'est pourquoi une destination comme Google est tout indiqué.

Modifier l'adresse IP

Pour modifer l'adresse IP vous devez modifier la ligne suivante:

RewriteCond %{REMOTE_ADDR} !^123\.123\.123\.121$

Si votre adresse IP est, par exemple, 255.255.255.255, la ligne deviendra:

RewriteCond %{REMOTE_ADDR} !^255\.255\.255\.255$

Ajouter une adresse IP

Pour ajouter une adresse IP (ex.: 255.255.255.255) vous devez ajouter la ligne suivante:

RewriteCond %{REMOTE_ADDR} !^255\.255\.255\.255$

Exemple avec 2 adresses IP:

```
RewriteEngine on
RewriteCond %{REQUEST_URI} ^(.*)?wp-login\.php(.*)$ [OR]
RewriteCond %{REQUEST_URI} ^(.*)?xmlrpc\.php(.*)$ [OR]
RewriteCond %{REQUEST_URI} ^(.*)?wp-admin$
RewriteCond %{REMOTE_ADDR} !^123\.123\.123\.121$
RewriteCond %{REMOTE_ADDR} !^255\.255\.255\.255$
RewriteRule ^(.*)$ http://www.google.ca [L,R=301]
```