Usamimi.info - サポート #218

海外からのアタックに対する予防策を考える

2015/09/11 10:34 - Clelia ごりゅ

ステータス:	終了	**開始日:**	2015/09/11
優先度:	通常	**期日:**	
担当者:	Clelia ごりゅ	**進捗率:**	100%
カテゴリ:		**予定工数:**	0.00時間
対象バージョン:		**作業時間:**	0.00時間

説明

概要

海外からの不正アクセスを防ぎ、usamimi.infoの環境を保護する
そうする事でサービスが止められてしまわないようにする

どのような理由があってもサービスが停止する事は、usamimi.infoの信用を損ねてしまうので
ユーザーさんに失望されないように注意しなければならない。

発覚までの経緯

つい先日に「usamimi.infoが少し重いかも？」といった早期警戒的な連絡を頂いたり
メインサーバーの通信量が増えていたり
負荷分散サーバーが頻繁に落ちたりと、少し怪しい雰囲気はあった。

しかしこの時点では、落ちた原因は夏の暑さでオーバーヒートしているか
負荷分散サーバーが落ちた事で通信にバタつきが生じて、重いように感じているのでは
といった感じであまり深く考えていなかった。

復帰させた負荷分散サーバーが1時間程度で再び落ちるといった異常な状態に遭遇した為
これは何か起きてそうな予感を感じ、負荷分散サーバーの主な仕事であるWEBサーバーのログをチェックしました。
結果、wp-login.phpへの大量のアクセスがある事が発覚し、これが原因となって過負荷で落ちている事が本当の原因であることが分かりました。

対策した内容

- ファイヤーウォール(ipfw)にIPを追加し、１つ１つアタックしてくるIPを除外するやり方
  結果は、IPをガンガン変えながらアクセスしに来たのでこちらでは対応しきれない状態になりました（マイナーな国ではジンバブエのIPとか。。。
- htaccess(apacheの設定)を使い、国単位でアクセスをブロックするやり方
  国単位ブロックの機能を使って、不正確セスの多い国ごとアクセスを遮断する
  効果はてきめんでしたが、日本以外からのアクセスがあるサイトもあった為
  弊害として正常なアクセスを排除してしまう事態が発生しました。
  - 国単位でブロックするのはPOSTのみに限定しGETや他のメソッドは制限しない
    最終的にはこのようにしました。

具体的な設定

apacheに対して以下の設定を施しています。

```
<Directory  />
        AllowOverride  None
        Order  allow,deny
        Allow  from  all

<Limit  POST>
  SetEnvIf  GEOIP_COUNTRY_CODE  CN  BlockCountry
  SetEnvIf  GEOIP_COUNTRY_CODE  ID  BlockCountry
  SetEnvIf  GEOIP_COUNTRY_CODE  RU  BlockCountry
  SetEnvIf  GEOIP_COUNTRY_CODE  KR  BlockCountry
  SetEnvIf  GEOIP_COUNTRY_CODE  TW  BlockCountry
```

```
  SetEnvIf  GEOIP_COUNTRY_CODE  FR  BlockCountry
  SetEnvIf  GEOIP_COUNTRY_CODE  UA  BlockCountry
  Deny  from  env=BlockCountry
</Limit>

<Files  "wp-login.php">
  Order  deny,allow
  Deny  from  all
  SetEnvIf  GEOIP_COUNTRY_CODE  JP  OkCountry
  Allow  from  env=OkCountry
</Files>
</Directory>
```

ユーザー側での制御

現状、Limit部分の物はOrderがallow,denyであるため（許可をチェックしてから、許可しないで絞る
幾ら許可を増やしても、許可しないを取り消せないと思います。

wp-login.phpはorderを変えてdeny,allowにしている為（許可しないをチェックしてから、許可するを追加する
許可する設定をhtaccessに追加してあげれば、後から制限を緩和できます。
Limitの方もその設定にしていった方がいいのでしょうかね。

具体例

```
<Files  "wp-login.php">
  SetEnvIf  GEOIP_COUNTRY_CODE  FR  OkCountry
  Allow  from  env=OkCountry
  Allow  from  192.168.0.111
</Files>
```

参考情報

レン鯖の中で有名な、さくらインターネットさんでは、アクセスを日本のみに絞るサービスを提供しているみたいです。
https://help.sakura.ad.jp/app/answers/detail/a_id/2258?_ga=1.222648539.1138274740.1441933429
無効にすることも可能ですが、デフォルトでは有効になっているみたいですね。
安全策なので、都合が悪くなければ有効にするべきだとは思います。
デフォルト無効だと、設定してくれるユーザーさんもいれば
放置してしまうユーザーさんもいる為、そこを攻撃される心配を考えれば、ですね

国単位アクセス制限について

GeoIPの機能を使って実現しています。
IP単位で管理する必要が無くなる為、大変助かっています。

以下はクレジット

この製品には MaxMind が作成した GeoLite2 データが含まれており、
http://www.maxmind.com から入手いただけます。

履歴

#1 - 2015/09/11 10:55 - Clelia ごりゅ

- 説明 を更新

誤字修正。。。

#2 - 2015/11/09 10:18 - Clelia ごりゅ

- ステータス を 進行中 から 終了 に変更

- 進捗率 を 0 から 100 に変更

アタックも落ち着きました（スパムメール送信問題など別のアタックが発生していますが）
チケットの内容をwikiへ記載しましたので
このチケットは完了として閉じます。