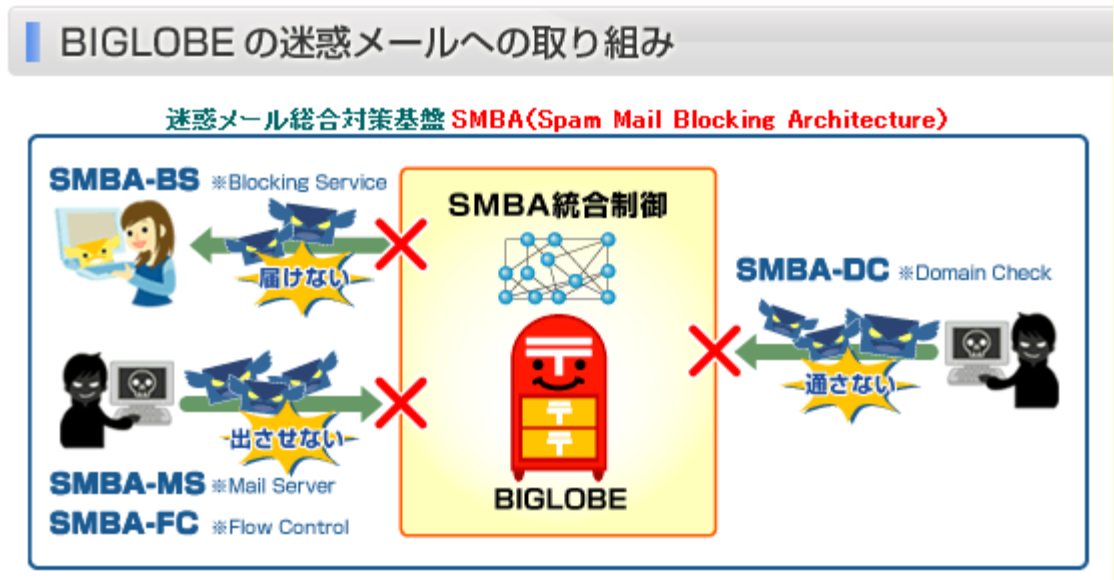
IAjapan 第10回
迷惑メール対策カンファレンス
ISPの対応事例～BIGLOBE編～

NECビッグローブ
加藤理人

2014/02/14

はじめに

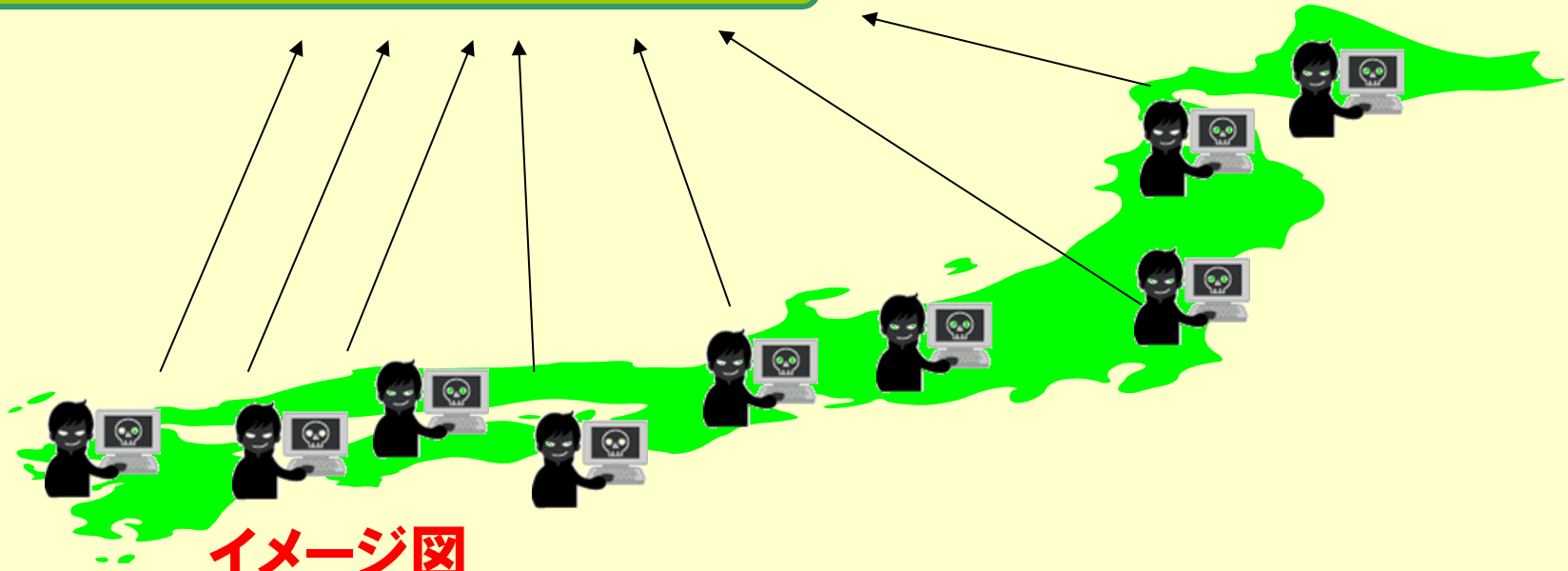
- Submission SPAMという迷惑メール送信方法がメールサービス提供者/システム管理者の共通課題となっています。
- BIGLOBEがこれまでに実施してきた各種SPAMメール対策をかいくぐり活発化しているSubmission SPAMに関し手口と現在の取り組みについてISPを代表して紹介いたします



これまでのSMTPアタックとは違います

BIGLOBE メール

アクセス集中で送信しづらい状況



イメージ図

Submission SPAM の傾向

- 2011年から規模拡大(発見は2009年)
- 主な送信元は海外のIPアドレス
- IPアドレスを素早く変えながら送信する
- 送信ポートは25/587等どれにも対応(WebメールのISPも)
- 主な送信宛先は海外のドメイン
- 認証してメール送信しているため、
  メールシステム管理者からは見分けられない
- 大量のアカウントが同時にやってくる
- 制限の上限を探るような送信もやっている
- POP/IMAPでメールボックスを見た形跡はない(今のところ)

Submission SPAMの構図

BlackListに登録される

送信メールの到着が遅延/不達

BIGLOBE メール

他社

サーバ高負荷、滞留アラーム発生

アクセス集中で送信しづらい状況

イメージ図

Submission SPAMが及ぼす影響（サポート/利用者）

サポート部門の負荷が増加

システム管理者　BIGLOBE カスタマーサポート

問い合わせ調査/回答

BlackList解除申請

アカウントが悪用されている

BIGLOBE 会員

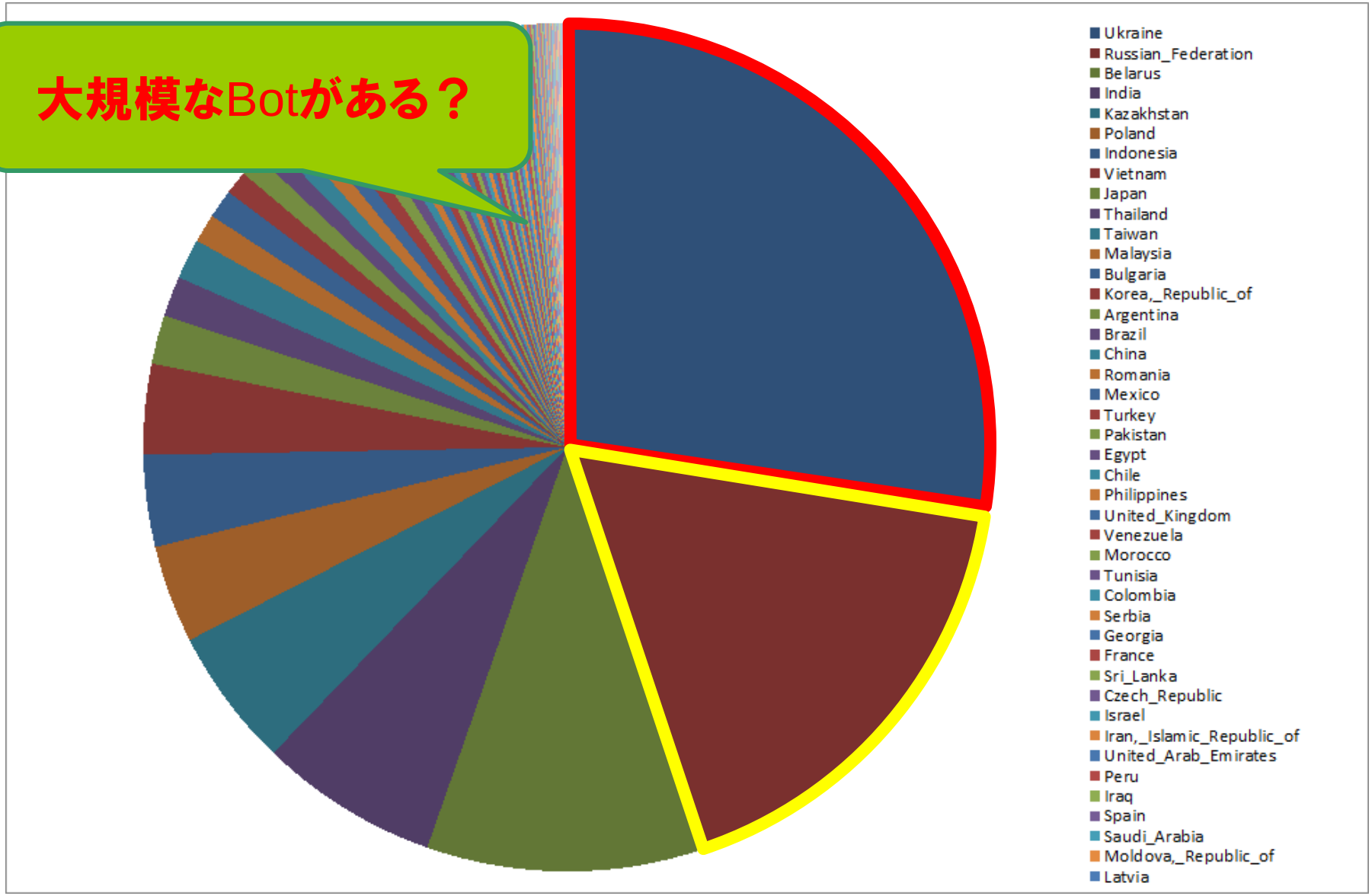
エラーメールがたくさん届いたのはなぜですか？

〇月〇日に大量にメール送信していますよ

SPAMメールを送信した心当たりがありません

送信したメールの到着に時間がかかっているようです

参考1：主な送信元は海外のIPアドレス



参考2：IPアドレスを変えながら送信する例

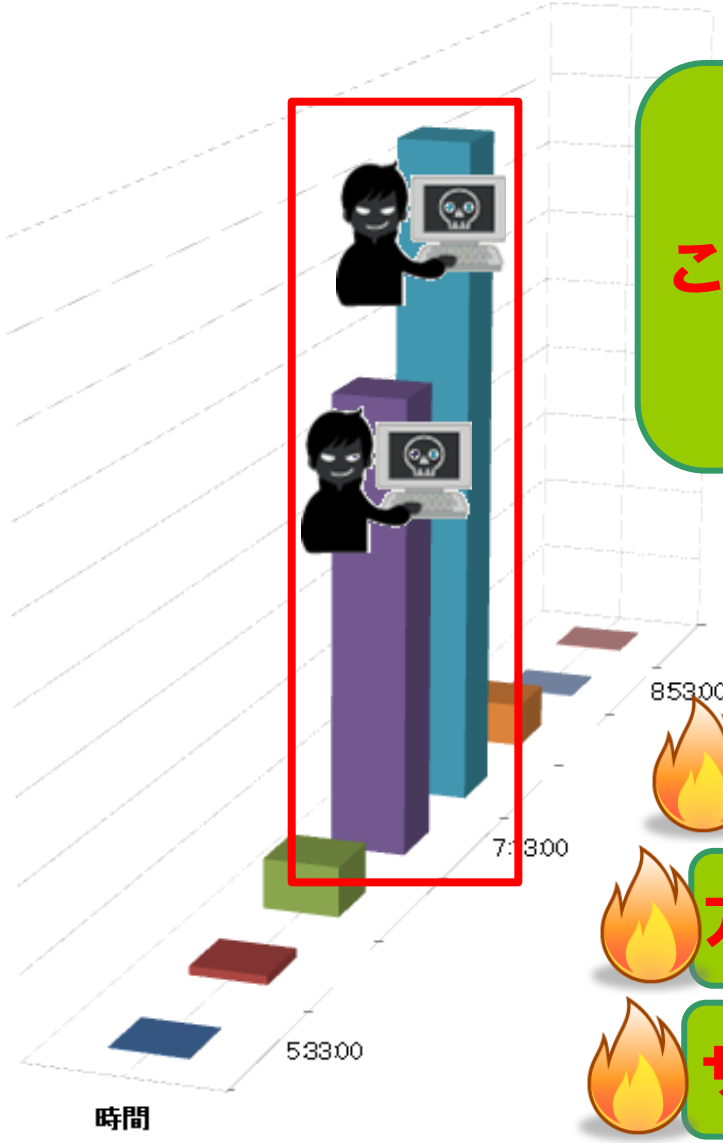
0:01:06	[176.212.202.226]	Russian_Federation
0:02:15	[46.119.249.144]	Ukraine
0:02:40	[178.120.124.232]	Belarus
0:03:43	[87.250.196.192]	Russian_Federation
0:06:04	[91.200.136.151]	Ukraine
0:06:27	[89.231.56.41]	Poland
0:06:35	[37.229.205.29]	Ukraine
0:07:42	[86.124.250.191]	Romania
0:10:27	[85.198.153.175]	Ukraine
0:11:44	[77.52.120.24]	Ukraine
0:14:03	[37.215.142.237]	Belarus
0:14:25	[176.101.234.168]	Russian_Federation
0:15:34	[46.118.8.161]	Ukraine
0:18:00	[5.139.3.182]	Russian_Federation
0:22:02	[119.14.132.57]	Taiwan
0:22:40	[122.166.224.104]	India
0:22:47	[37.213.213.97]	Belarus
0:23:59	[85.198.162.9]	Ukraine
0:26:25	[46.61.126.99]	Russian_Federation
0:28:12	[176.102.206.166]	Ukraine
0:30:42	[93.170.149.188]	Czech_Republic
0:31:28	[91.214.133.77]	Ukraine
0:32:56	[46.181.68.22]	Russian_Federation
0:37:18	[176.212.202.226]	Russian_Federation
0:37:55	[95.132.29.153]	Ukraine
0:39:38	[188.186.151.147]	Russian_Federation
0:40:31	[178.125.64.164]	Belarus
0:42:24	[178.122.186.149]	Belarus
0:44:16	[117.199.216.44]	India
0:45:27	[36.73.115.179]	Indonesia
0:46:26	[92.126.102.97]	Russian_Federation
0:48:57	[5.128.26.206]	Russian_Federation
0:49:20	[220.143.186.43]	Taiwan
0:50:10	[61.228.152.91]	Taiwan
0:50:39	[109.86.30.244]	Ukraine
0:53:54	[223.182.207.115]	India
0:54:07	[188.233.227.94]	Russian_Federation
0:54:45	[200.82.66.166]	Argentina
0:54:55	[31.135.250.154]	Kyrgyzstan
0:58:44	[188.232.90.69]	Russian_Federation
0:59:04	[94.41.38.229]	Russian_Federation
0:59:50	[46.202.24.224]	Ukraine

1:02:49	[134	
1:04:03	[46.	
1:04:36	[89.2	
1:05:13	[93.1	
1:06:45	[176	
1:09:29	[93.	
1:10:24	[202	
1:10:36	[115.242.132.202]	India
1:14:37	[188.191.22.42]	Ukraine
1:14:37	[188	
1:14:50	[188	
1:15:57	[94.4	
1:19:06	[178	
1:20:43	[93.8	
1:21:01	[182	
1:22:06	[93.7	
1:23:25	[213.87.85.247]	Russian_Federation
1:26:29	[188.186.147.10]	Russian_Federation
1:26:44	[5.58.44.10]	Ukraine
1:27:39	[188.234.22.91]	Russian_Federation
1:28:08	[188.235.67.106]	Russian_Federation
1:31:52	[46.35.244.230]	Ukraine
1:32:16	[178.64.51.43]	Russian_Federation
1:32:24	[93.74.115.121]	Ukraine
1:36:16	[31.135.114.37]	Russian_Federation
1:38:13	[46.0.116.83]	Russian_Federation
1:38:20	[186.55.10.29]	Uruguay
1:40:16	[81.163.143.38]	Ukraine
1:40:57	[110.8.163.2]	Korea,_Republic_of
1:44:19	[83.237.126.18]	Russian_Federation
1:44:22	[46.242.32.216]	Russian_Federation
1:46:14	[178.123.56.143]	Belarus
1:46:36	[193.138.176.22]	Russian_Federation
1:50:34	[95.67.249.187]	Russian_Federation
1:50:57	[176.100.166.203]	Ukraine
1:51:05	[178.172.228.182]	Belarus
1:52:58	[79.183.17.154]	Israel
1:56:56	[46.118.174.249]	Ukraine
1:57:16	[37.193.216.129]	Russian_Federation
1:59:23	[91.193.233.45]	Ukraine
2:00:40	[95.182.80.41]	Russian_Federation
2:03:25	[176.8.142.25]	Ukraine

国内からの送信が無い

送信時間が重ならない
同時送信制限を回避？

参考3：大量のアカウントが同時にやってきた例



突然大量にやってきた
この日の制限上限まで送信された
繰り返し悪用される(翌日に)

- BlackListに登録される
- 送信メールの到着が遅延/不達
- アクセス集中で送信しづらい状況
- サーバ高負荷、滞留アラーム発生

現在の取り組み内容

1.Submission SPAM検出

2.対象アカウントの送信停止

BIGLOBE
カスタマー
サポート

手間のかかる対症療法を
続けています

1週間程度
(平均)

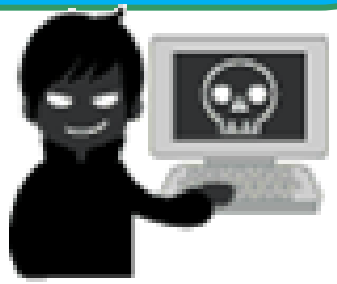
BIGLOBE
会員

3.送信停止の連絡
・ウイルススキャン
・パスワードの変更

4.会員からの返答
・ウイルススキャン済
・パスワードの変更済

5. 送信停止の解除(即時)

6.送信停止解除の連絡(即時)



7.あとで元のパスワード
に戻す会員もいて
再度悪用される

再発

まとめ1

- Submission SPAMは会員のアカウントで認証してSPAM送信されるので
  - 効果的な防止策が取りにくい
  - メールシステム管理者が気づいたときは手遅れになっている
  - ドメインのレピュテーションが悪化してしまう
- 認証エラーは増えていないので

  エラーの多いアカウント/アクセス元探しは効果が低い
- 送信元IPが広範囲かつすぐ変わるのでフィルタが困難
- サポート部門の負荷が増えている
  - 毎日これだけやっている人がいます・・・
  - 法人サービスは事前連絡必要だったり・・・

今の対処法はもう限界

サービスレベルの維持も困難

まとめ2

- 発見方法
  - ISPの立場では送信の振る舞いから判断するしか
- 発見時の対処
  - 強制的な送信停止をしてよいか判断に悩む
- 今後の防止策
  - システム側

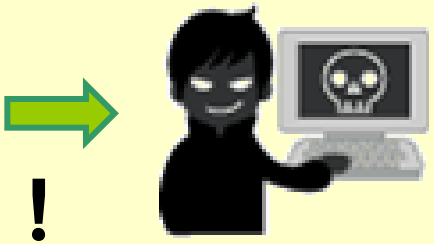
    コンテンツスキャンしか手段がない？

    SSL/TLS/HTTPSを提供する効果は？
  - 利用者側

    各種サイトでパスワードの使い回しは避ける、他に何かできることは？

おわり

そもそもはこれを何とかしたい



TREND MICRO Symantec. さん期待しています！

以上です
ありがとうございました