日本がスパム発信元でなくなるためには
～続・Submission 踏み台問題～

2014年10月8日

講師： 阿部敏一（OCN）
講師： 島村充（IIJ）
コーディネーター： 加瀬正樹（ニフティ）

アジェンダ

- ✓ Submission **踏み台問題の振り返り＆**Update
- ✓ **コンシューマ向けメールでの状況・対策・課題**
- ✓ **エンタープライズ向けメールでの状況・対策・課題**
- ✓ **会場からのご意見・ご質問**

前回(２月)のセッションを振り返ります

@nifty

- submission **踏み台問題とは・・・**
  - ID/PW**入手→スパム発信→**BlockList**登録→お隣さん問題**
  - 2009**年ごろから発生**
  - **大量のアカウントから送信される(**IDかんじきスパム**)**
  - **海外**IP**アドレスが発信元(今のところ)**
  - **サポート部隊の負荷が心配**

- ID/PW**はどうやって入手しているのか・・・**
  - **マルウェア経由と思われる**
  - **スパム＋ウイルスメールが増加傾向**
  - **スパム発信だけでなくアドレスリスト入手も**

前回(２月)のセッションを振り返ります

@nifty

・対策案
- ID/PW入手 → オンライン攻撃対策、危殆化システム廃止
- スパム発信(入口) → 従来のピッチコントロール
  ただし、Auth ID ベース
- スパム発信(出口) → 出口IP/MTAの分離
  MSAでのコンテンツフィルタリング
- その他 → ワンタイムPW、マルチ要素認証、原則送信禁止
  ただし、海外IP等といった一定の条件下

Update（ガイドラインの改訂）

電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン（2014年7月22日）

http://jaipa.or.jp/other/mtcs/guideline_v3.pdf

【事例①】
攻撃者がSMTP認証のID・PWを不正に利用して迷惑メールを送付し、メールの遅配が発生したため、送信元IPアドレス、タイムスタンプ、メールアドレス、認証IDを分析して、瞬時に別の地域に移動してSMTPしている蓋然性が高いと確認できたため、ユーザに個別連絡・パスワード変更を依頼した。

【事例②】
大量のSMTP認証の失敗ログが見つかり、ID・PWの不正利用の可能性が考えられたため、発信元IPアドレス、タイムスタンプ、認証回数、認証間隔を分析して、アカウントの不正取得をしている蓋然性が高いと確認できたため、当該IPアドレスからのSMTP認証を停止した。

Update(スパム発信数・停止措置件数)

メモ禁止

@nifty

当日限り

事業者2社からご登壇いただきました

＜コンシューマー向けメールシステム＞

阿部　敏一

NTTコム ソリューション&エンジニアリング株式会社

＜エンタープライズ向けメールシステム＞

島村　充

株式会社インターネットイニシアティブ

会場からのご質問・ご意見