IP Meeting 2013
午後の部:荒ぶるインターネットを乗りこなす
「Internet Week 2013 最新動向セッション」の総括から見る、2013年のインターネット

【S2】DDoS攻撃の実態と対策

佐藤 友治
（インターネットセキュリティ（元）専門家）

- 2013年の3月の、Spamhaus への攻撃でそのトラフィク量が話題に。
- 同時にDNS amp攻撃とOpenResolver 問題が再浮上。
- 海外では対策製品、サービスの市場が伸びている(らしい)
- ハクティビスト

なぜ、今DoS/DDoS対策が注目されたのか。

ところが

- 海外で大きな被害報道を目にするが、日本の企業やサービスでインパクトのあるDDoS攻撃の報道はあまり一般の話題にのぼらない。
- ネットワークオペレータ以外の人が攻撃トラフィック傾向を知る機会が意外と少ない。
- DNS amp攻撃って自分に関係あるのか？

参加者

- 申込者:99名
- 参加者傾向
  - インターネットのトラフィック、パケット傾向をキャッチアップしにくい層
  - これまでのIP Meeting に馴染みの薄い層

講師

- 佐々木崇
  - Arbor Networks
- 井上 大介
  - 独立行政法人情報通信研究機構 ネットワークセキュリティ研究所 サイバーセキュリティ研究室 室長
- 高田美紀、西塚 要
  - NTTコミュニケーションズ

攻撃傾向

- 2010年から2013年のトラフィックベースの傾向
  - bps (bit per second) ベースは増加
  - pps (packet per second)は下がってきていたが、2013年は上昇
  - 2013年はロングパケットの攻撃が増えた。
    - IP Meeting午前のトラフィック傾向の報告と違いがある。
  - 短時間化
    - BotネットのDDoSツールのお試し版を使う
    - 攻撃の対策を打たれる前に、つかまらない程度にやめる。
- 複数ベクトルによる攻撃手法
- パケット・フラグメント化　port0の攻撃

攻撃傾向(2/2)

- Googleデジタルアタックマップ（DDoS攻撃）が公開される。
  - http://www.digitalattackmap.com
  - Arbor Networksと協力
- フランスが攻撃先国第3位に
  - データセンターが多く立ち上がったためではないか。
- 日本への攻撃パケット量は横ばい。
  - 平均866.4Mbps
  - 最大　6.71Gbps
- 2013年日本への攻撃パケットの最大
  9月18日　58Gbps（複数のホストへの合計）

- Googleの検索で簡単にみつかる
  - オンラインゲームで相手のPCを攻撃するのにも使うらしい。
- Android版もある
  - 20Mbpsでるらしい。

DOSツール

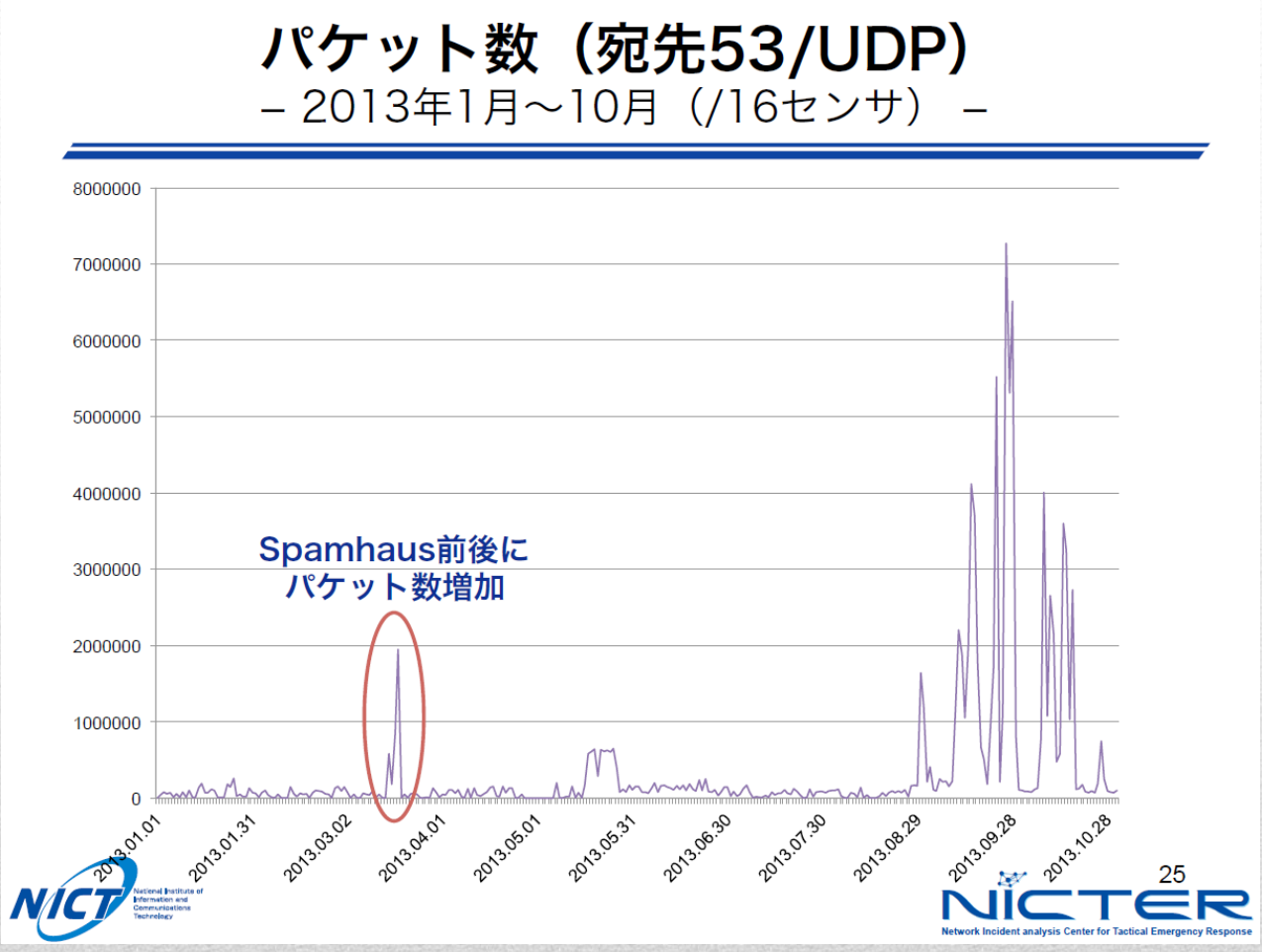
ビジュアル化

- 攻撃パケットをビジュアル化して見せるサイトが複数公開される。
- Digital Attack Map
  - http://www.digitalattackmap.com/
  - Arbor Networks と Google のコラボ
- nicter /DAEDALUS
- SAMURAI

- アイドルグループ「アフィリア・サーガ」のPVの背景に注目

http://www.youtube.com/watch?v=pY-HaHWjbgk

こんな使われ方も



のらOpenResolver探し

- 一年間の攻撃トレンドはこれまで通り、分析と対策を提案して欲しい
- 各ISP事業者が連携した対策、総務省等への働きかけを積極的に行う機会を作ってほしい。
- 攻撃と対策の手法が高度化していることがわかりました。
- DNS amp攻撃の威力がわかった。
- DDoS対策 HowToの紹介
- 防御手法についてもう少し大きく取り上げて欲しい
- 対策面にフォーカスした話が聞けたらよいと思った。
- 色々な事例が聞けて興味深かった。
- 実際にどう防御をすればよいのか？
- 日本の攻撃状況を知りたい。
- 日常の対策として、どのような調査対策がとれるのか？
- サーバ側での対策
- 特定の被害社に関する詳細な事例を聞いてみたい
- DDoS停止の判断などの運用ポイントなどテクニック
- 情報を共有することで認識レベルがあがります。
- 商用ダイダロスに関して
- 装置の紹介
- もっと最新の攻撃状況の報告と対策例が知りたかった。

アンケートより（集計前）

見送ったネタ

- BGP Flow Spec
- RFC 5575
  - Dissemination of Flow Specification Rules
- RFC5675
  - Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)
- CloudFlare pins outage on bad rule for Juniper routers（副作用）
  - http://www.zdnet.com/cloudflare-pins-outage-on-bad-rule-for-juniper-routers-7000012084/
  - CloudFlare　無料のCDN