DDoSターゲットになったら

What if you are a DDoS target?

東京大学情報基盤センター

Information Technology Center, the Univ. of Tokyo

安東孝二

Koji ANDO

<chutzpah@itc.u-tokyo.ac.jp>

<chutzpah@apache.or.jp>

自己紹介

- 東京大学情報基盤センター所属
- 普段はアプリケーションレイヤー
- ネットワークの専門オペレータではない、が….
- JPCERTに対抗してUTCERT

DoS,DDoSってなに？

- Denial of Service
  - 一般には正面玄関から客が1万人来る状態
- Distributed Denial of Service
  - 某掲示板を見た日本中の2ちゃんねらーが、正面玄関から10万人入ってくる状態

DDoS versus DoS

- メールで考えてみる
  - 一箇所からたくさん ⇒ DoS?
  - 複数箇所から同時にたくさん ⇒ DDoS?
- McDonald's で考えてみる
  - 一店舗で100円バーガーをたくさん買う⇒DoS
  - 富山市内の12店舗で同時期に100円バーガーをたくさん買う⇒DDoS
    - 近所の店舗に在庫を取りにいけないので破綻する

DDoSとDoSのいやらしさの違い

- たとえばメール
  - bulk mailが一箇所から来る場合
    - SMTPのアクセスをとめればおしまい
  - 世界中のopen relayサーバーから来る場合
    - 統一的な対処は不可能
- DDoSのほうがいやらしい
  - DoSはシンプルな力技
  - DDoSはパラレルな工夫？をした力技

そもそもDoS-like話はよくある

- 東京大学情報基盤センターの５年前
  - 3,500人メール事件
  - メールピンポン
- 年2回の有明方面の交通機関
- あけおめコール
- etc.

DDoSの大きな分類

- JANOGなのでServiceをネットワークレイヤーに限定してみると….
  - ルーターCPUひぃひぃ系
  - バンド幅食いつぶし系
    - 命名　かとうあきら
- パケットを増幅する仕組みが悪用される？
  - ip directed-broadcast

smurfの記録@東京大学

- 経緯
  - 学内の遠隔キャンパスからメールが届かない、DNSも引けないとの報告
  - メインキャンパス本郷との間の帯域があふれている
  - とりあえずダンプする
  - 大量のICMP echo replyが世界中から
  - ターゲットマシンはIRCサーバー

smurfの記録＠東京大学

- 帯域食いつぶし系DDoSアタックと判断
- Sinet経由で国内を含む数百箇所から
  - Sinetというくらいで、promptな対処は望めない
- どうもbroadcast echo replyをしているルーターをうまく使っているらしい（いわゆるsmurf）
- 国内の一部の大学には連絡
- さて、どうしよう

smurfの記録@東京大学

- 幸いにも食いつぶしているのは学内の網のみ
  - icmp echo replyだけで70Mbpsくらい
- 対外線には余裕があった
- icmp echo reply全部をブロック？
  - 副作用は？
- ルーターでACLを適用？
  - ルーターがひぃひぃ言うかも

smurfの記録@東京大学

- 対策
  - ICMP echo replyだけ遅いネットワークを作る
    - policy routingでicmp echo replyを分ける
    - ルーティングした先で、10MbpsのHUBに突っ込む
    - 自然にshaping?

DDoSを受けて一瞬思ったこと

- DDoSを避けることはできないかも
- 対応方法に王道はないだろう
- さぁ、これからどうする？
  - SuperSinetは10Gbpsです:-)
  - ブロードバンドな一般家庭も集まると怖い
    - 数の暴力はそれなりに怖いです
  - CodeRedなどのウイルスを用いられたら……
    - ホワイトハウスの例

これからのDDoS対策

- 各種アタックの複合体の一部としてのDDoS
  - CodeRed,Nimda
- ネットワークレイヤーだけではだめかも
  - specialist & generalist
  - 政治層？宗教層？