DNS amplification attacks

Matsuzaki Yoshinobu
<maz@iij.ad.jp>

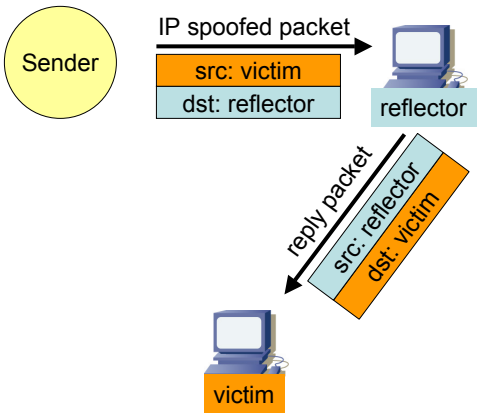
DNS amplification attacksとは

- 送信元を偽装したdns queryによる攻撃
  - 帯域を埋める
  - ‘smurf attacks’に類似
- 攻撃要素は
  - IP spoofing
  - DNS amp

IP spoofing + DNS amp

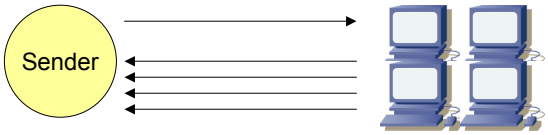
- IP spoofing
  - 送信元IPアドレスを偽装したdns query
  - 反射パケットを利用するため
- DNS amp
  - UDP (簡単に利用できる)
  - 大きな増幅率 =~ 60 (EDNS0の利用)
  - リゾルバ (dns cache)による分散

反射(reflection)

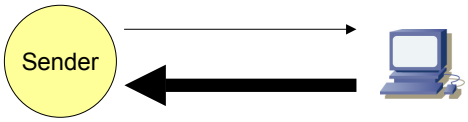


増幅(amplification)

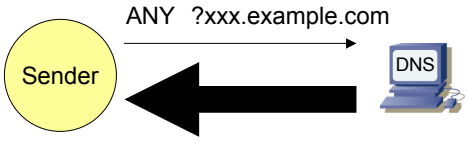
1. multiple replies



2. bigger reply

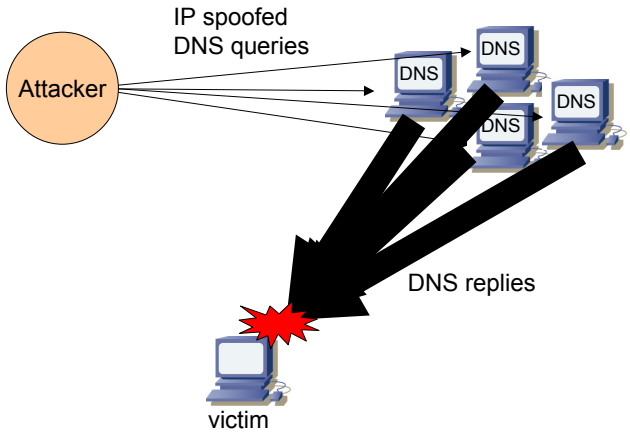


DNS amplification

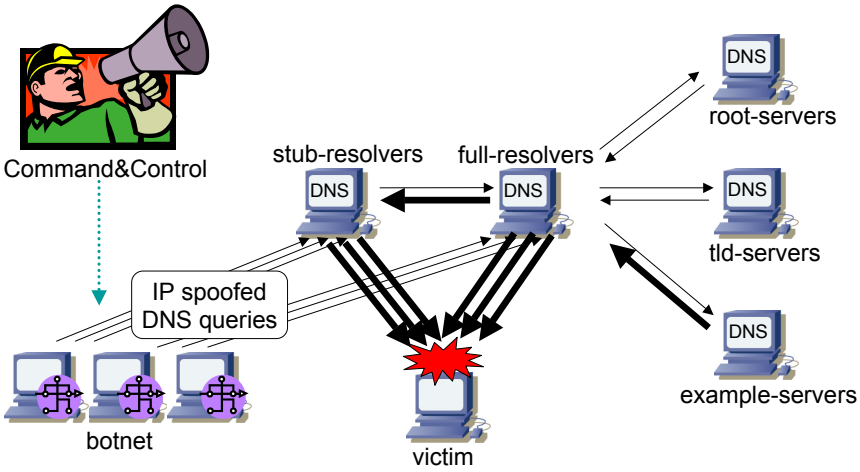


xxx.example.com IN TXT
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX

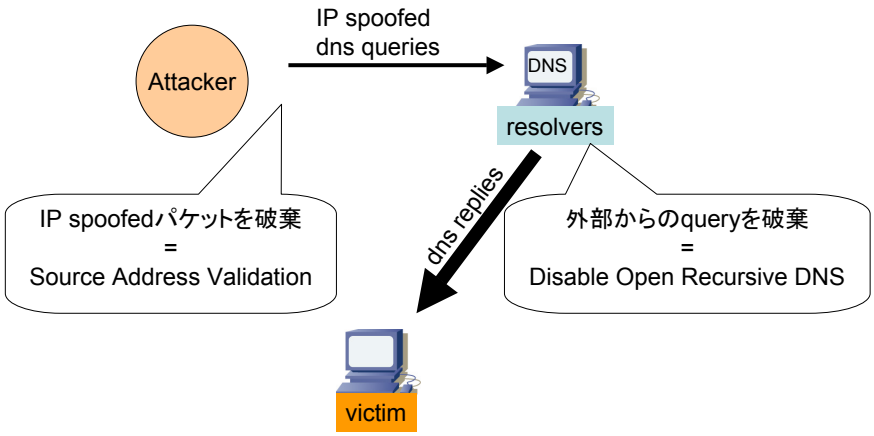
DNS amplification attack



攻撃の相関関係



対策



Disable Open Recursive DNS

- ‘open relay’なリゾルバがいっぱい
  - ISPのDNSサーバ
  - 各組織のDNSサーバ
  - 幾つかの、ちょっと賢い機器
- 必要な範囲にだけサービスを提供しましょう
  - コンテンツサーバを兼ねている場合は要注意

Source Address Validation

- 送信元IPアドレスを検証すること
  - 不正な送信元IPアドレスをフィルタ
  - できるだけ生成元の近くでフィルタ
  - できるだけ厳密なルールでフィルタ
- 全てのネットワークで実装されれば、ip spoofingを悪用した活動を根絶できる
  - BCP38とBCP84は必読

Source Address Validationの実装

- ACL
  - 状態を持たず、決定的
  - 更新に注意
- uRPF
  - 経路テーブル依存
  - 経路さえ正しく保てばよく動く
  - 幾つかのモード (strict/loose/feasible/VPN?)

参照先

- AL-1999.004 – DoS attacks using the DNS
  - http://www.auscert.org.au/render.html?it=80
- The Continuing DoS Threat Posed by DNS Recursion
  - http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf
- SAC008 – DNS Distributed DDoS Attacks
  - http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf
- DNSの再帰的な問い合わせを悪用したDDoS攻撃手法の検証について
  - http://www.cyberpolice.go.jp/detect/pdf/20060711_DNS-DDoS.pdf

おわり