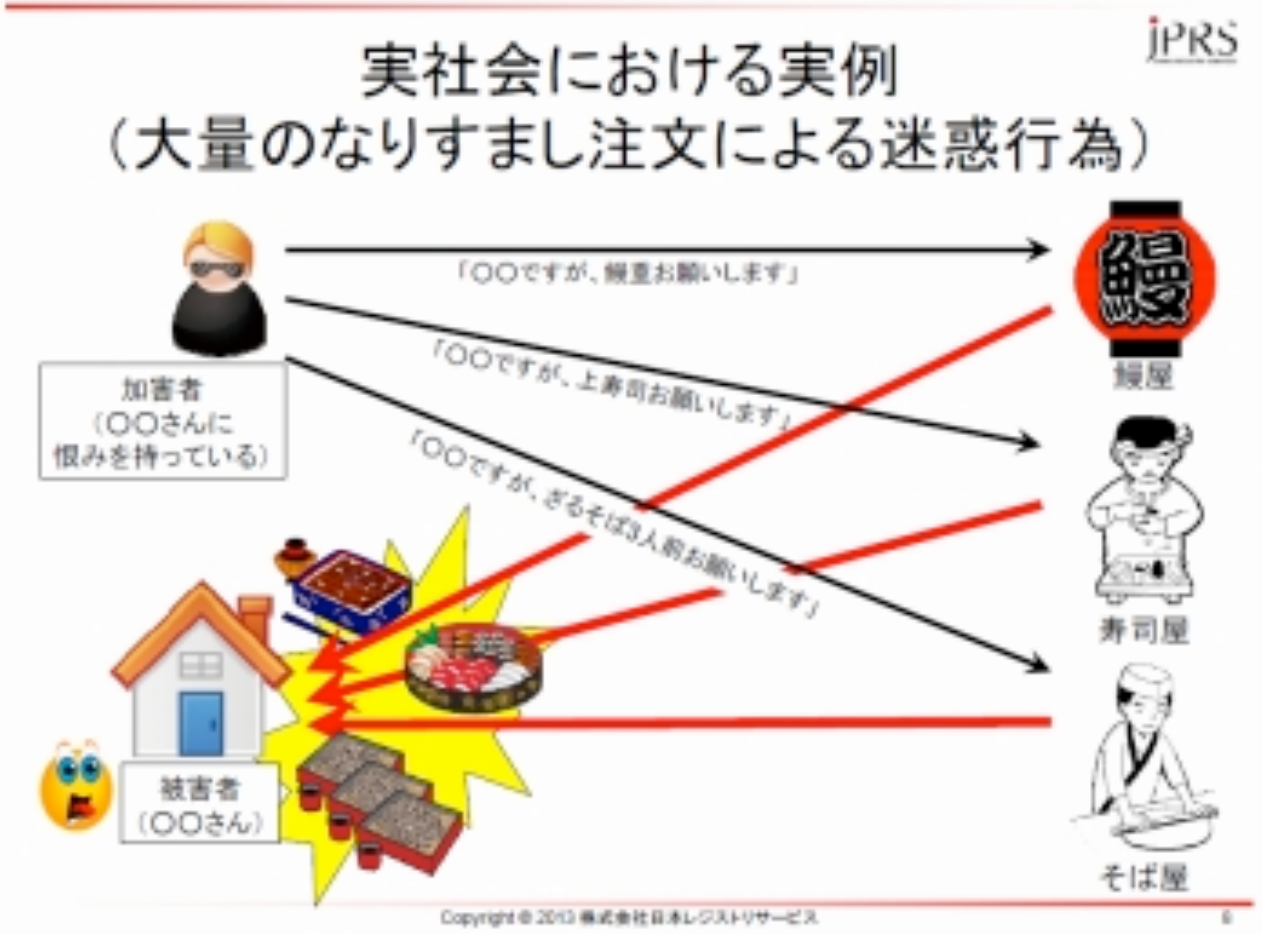
DNSオープンリゾルバ問題

やまぐちたかのり

身元詐称による迷惑行為



– http://internet.watch.impress.co.jp/docs/interview/20130426_597628.html

なりすまし攻撃

- Smurf
  - ICMP echo でブロードキャスト
- Land
  - TCPのSYN+ACK パケットを自分自身に投げさせることで無限ループ
- SYN flood
  - 大量のTCP SYNパケットを送って、その応答のSYN+ACKを無視する
- Backscatter (NDR spam)
  - 存在しないアドレス宛にメールを送信し、その結果発生したバウンスメール(NDR)を詐称されたメールアドレスに送りつける
- いずれも送信元アドレスを詐称することによる攻撃
  - backscatterはメールアドレス、それ以外はIPアドレス

DNS amp (1)

- DNSを使ったなりすまし攻撃
  - 送信元アドレスを詐称してDNS問い合わせを送ると、詐称されたアドレスに応答が返る
    - TCPと違ってUDPは接続元を確認しない
- 詐称したIPアドレスに大きなDNS応答を返させる
  - DNSは問い合わせよりも応答の方がかならず大きくなる
    - 攻撃者がうまく調整すれば増幅率が50倍～100倍以上に
  - 効率的にネットワークを飽和させられる
    - botnet でさらに効率的に

DNS amp (2)

- ホストの脆弱性を狙う攻撃ではない
  - 既知の脆弱性をすべて対策していても防げない
  - ネットワークを飽和させる攻撃
    - 大量のトラフィックで帯域を埋める
    - 詐称されたIPアドレスを持つホストが存在していなくても、経路が存在していれば、そのネットワークに大量のパケットが流入して飽和する
- DNSというより、UDPであることが本質
  - TCP上のDNSでは成立しない
  - DNSでなくても、SNMPやNTPなどでも成立する
    - http://www.prolexic.com/kcresources/white-paper/white-paper-snmp-ntp-chargen-reflection-attacks-drdos/index.html

オープンリゾルバとは?

- アクセス制限のかかっていないフルサービスリゾルバ
  - フルサービスリゾルバ: キャッシュDNSサーバとかDNS fowarderとかの名前解決用サービス
  - スタブリゾルバ: getaddrinfo(3) などのライブラリ関数(API)
- 誰でも利用できてしまうので、任意の標的に対するDNS amp攻撃の踏み台に利用されうる
  - アクセス制限すべし
- Open Resolver Project によると、2800万台も存在するって…!
  - http://openresolverproject.org/breakdown.cgi
  - カウント方法はわりと問題あるっぽいが

攻撃事例

- 2013/5 Prolexic 167Gbps
- 2013/3 Spamhaus/CloudFlare 300Gbps
  - 今年になってこの話題が注目されてるのはこれの影響
- 2010/3 2ちゃんねる
- 2006/2 ルートサーバ、TLDネームサーバ 2.5Gbps
- 公表されてないだけでほかにも無数の事例
- 手法自体は1999年ごろには見つかっていたらしい
  - http://www.auscert.org.au/render.html?it=80

どうやれば防げる?

- 攻撃を受けている側での対処は非常に困難
  - 標的のネットワークにすでに届いてしまっているパケットは、もうどうしようもない
  - パケットを捨てる以外のことはできないが、量が多いと捨てるにも負荷が大きい
  - パケットの送信元にできるだけ近いところ(境界ルータ)でフィルタ
    - ネットワーク内のトラフィックが飽和して他の通信が阻害されないように
    - 大量トラフィックの影響を受ける機器の数を減らす
- 攻撃者にアドレス詐称クエリをやめさせる
- ampの踏み台に応答をやめさせる
  - いずれも被害者がみずから実施できる対策ではない

キャッシュDNSサーバ

- ISPごと、会社ごと、組織ごとに用意
  - その組織に属するメンバー向け
  - 属さない人に機能を提供する必要はない
- 組織内からのアクセスだけを受けて、それ以外は無視しても困らない
  - 知らないところからのクエリは捨てる
  - 送信元詐称クエリも捨てるので、増幅応答を返さなくなる
  - 組織内のアドレスに詐称されると応答を返すが、応答先は組織内なので、外部に迷惑をかけることはない

ブロードバンドルータ

- たいていDNS forwarder機能を持つ
  - クライアントからのDNSクエリを指定されたキャッシュサーバに転送
- 設置してある宅内でだけ使えればよい
  - WAN側からの問い合わせを受ける必要はない
- LAN側からのみアクセスできるようになってるか設定を確認
  - 設定変更できない機種ならファームウェアのバージョンアップで対応できないか確認
  - それもダメならDNS forwarder機能をoff
    - 各PCに個別でISPのキャッシュサーバのアドレスを設定
      - 手動設定は推奨されないが、やむなし
    - むしろ買い替えるべし

DNS cache poisoning

- 嘘の情報をキャッシュさせる攻撃
- 本来の権威サーバからの応答が届く前に、偽造応答をキャッシュDNSサーバに注入する
- DNSプロトコルそのものの脆弱性
  - オープンリゾルバでなくても防げない
- オープンリゾルバでは、誰でもキャッシュDNSサーバにクエリを送りこめる
  - 偽造応答を送りつけるタイミングの制御が容易
  - とはいえ、クエリの送信元偽造もまた容易なので、アクセス制限されているから困難というわけでもない

BCP38

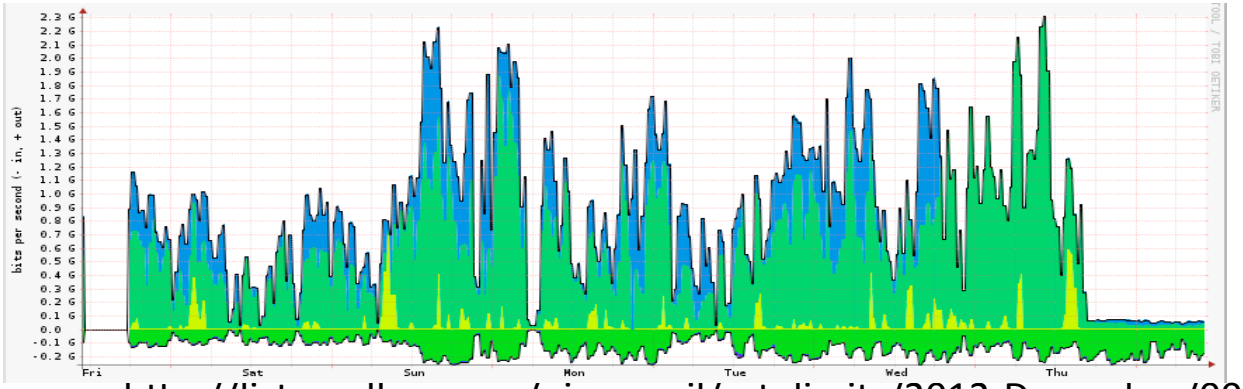
- Ingress Filtering (RFC2827)
- よそのネットワークのIPアドレスをsrcとするパケットを、自分のネットワークに外に出さないようにフィルタする
- アドレス詐称パケットそのものが出なくなるので、根本的な対策になる
  - SYN floodその他多くのなりすまし攻撃も止められる
    - メールのなりすましspamは止められないけど
- が、ampの踏み台となっているDNSサーバでこれをやっても効果なし
  - 攻撃元のネットワークで対処されるべき
- 利他的な設定で、自分のメリットが薄いので導入が進まない
  - とはいえ、ボットが意図せず攻撃することを防げるのでやるべき

権威DNSサーバ

- ゾーン情報を登録するサーバ
- DNSの応答を返すので、やっぱりDNS ampの踏み台に使える
- キャッシュDNSサーバと異なり、アクセス制限は困難
  - リゾルバではないので、オープンリゾルバとは呼ばない
- 攻撃者が任意の情報を登録するのは困難
  - 踏み台として利用することは簡単だが、攻撃者の側で増幅率を大きくしようと操作することはできない
  - キャッシュサーバは外部の情報をコピーしてきてキャッシュするので、コピー元のサーバを攻撃者が用意すればいい
- DNSSEC
  - 署名が付加されるのでサイズが大きくなる
  - 攻撃者がわざわざ仕込まなくても、大きな増幅率が得られる

レート制限

- 大量の問い合わせを出しているクライアントには応答しない
- amp の踏み台にならないわけではないが、緩和される
- アクセス制限できない権威DNSサーバでのamp対策手法
  - Afilias (.orgのレジストリ)で2.3Gbps → 70Mbps



  - http://lists.redbarn.org/pipermail/ratelimits/2012-December/000144.html
- キャッシュサーバで導入しているところもある
  - Google Public DNS (8.8.8.8/8.8.4.4)

まとめ

- DNS ampヤバイ
- オープンリゾルバいっぱい
- 攻撃事例いっぱい
- 直すのたいへん
- 道は険しい