NTT

NTT Information Sharing Platform Laboratories

DNSキャッシュ汚染攻撃

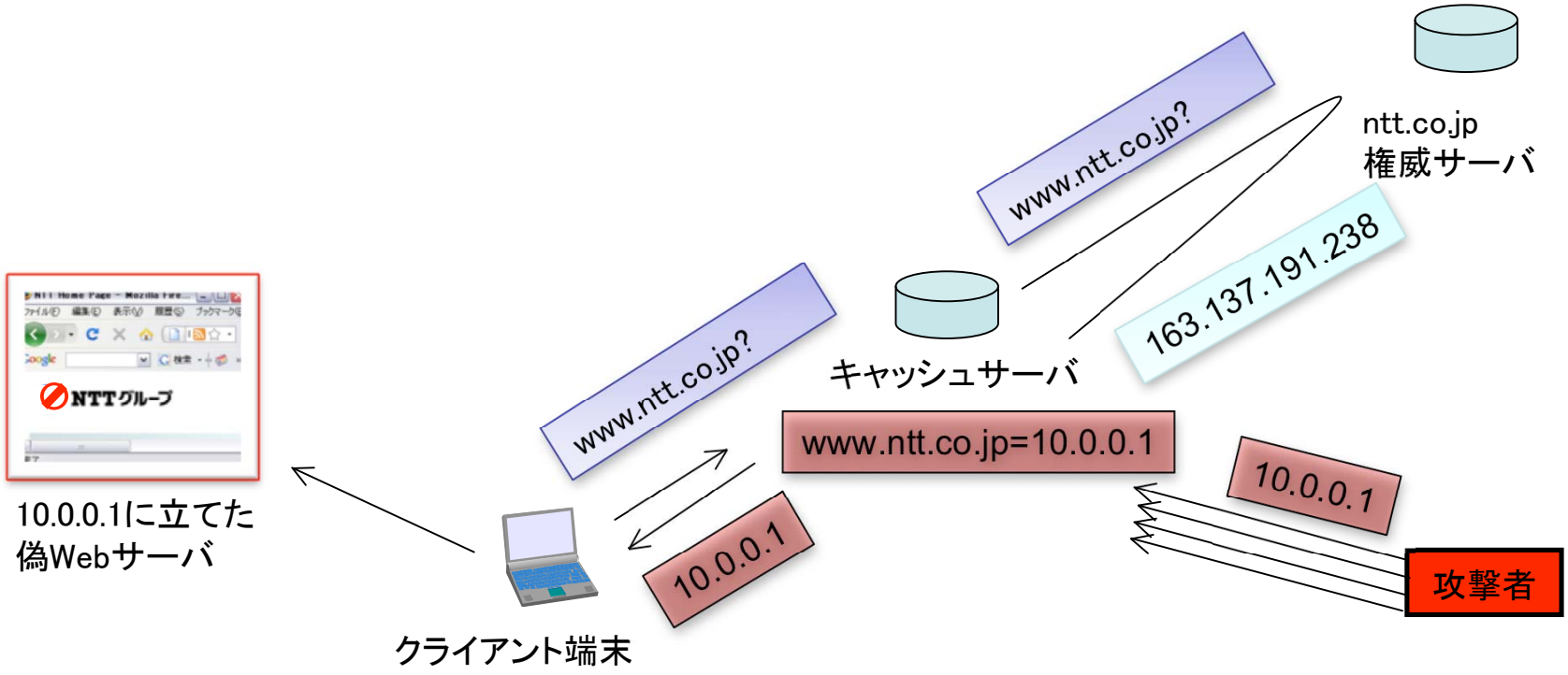
2008/12/17

NTT情報流通プラットフォーム研究所

NTT Information Sharing Platform Labs.

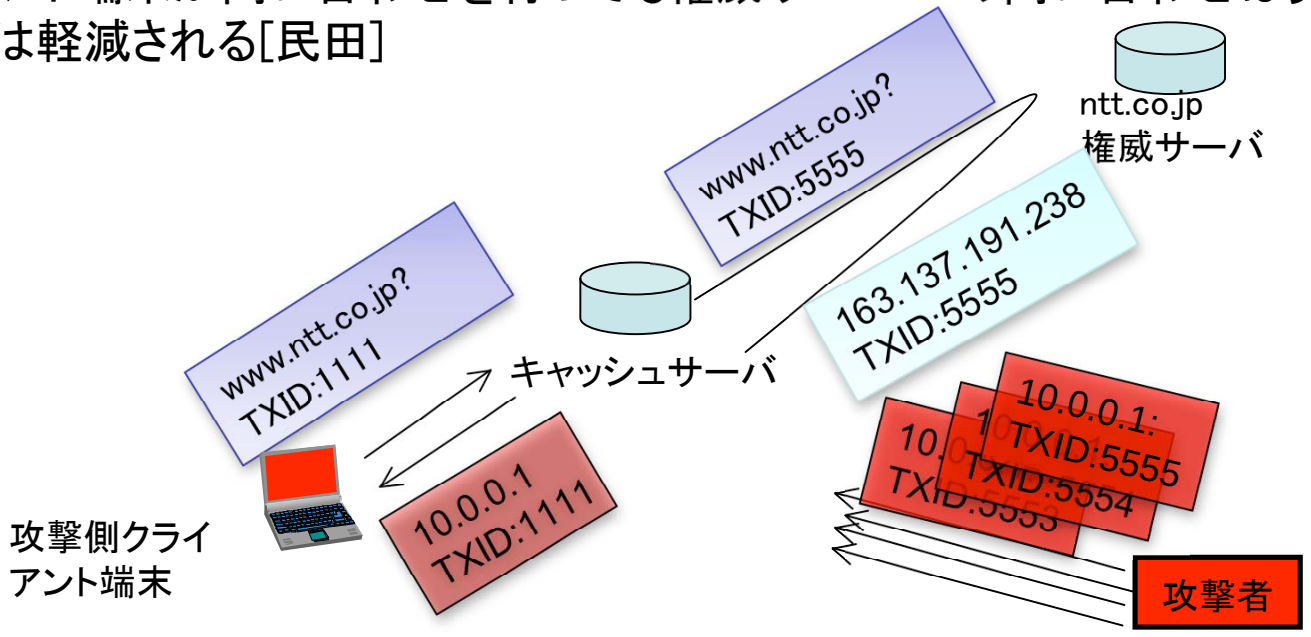
DNSキャッシュ汚染(1/3)

- DNSの名前解決：クライアント端末は通常，問い合わせドメイン名を管理するDNS権威サーバに直接問い合わせを行わず，DNSキャッシュサーバが問い合わせを行う．
- DNSキャッシュ汚染：DNSキャッシュサーバがキャッシュするドメイン名のレコードとして偽のIPアドレスを注入する
- ゾーンごと乗っ取られる可能性もあり
  - .google.com, etc
- クライアントのアクセス先を自由にコントロールできる



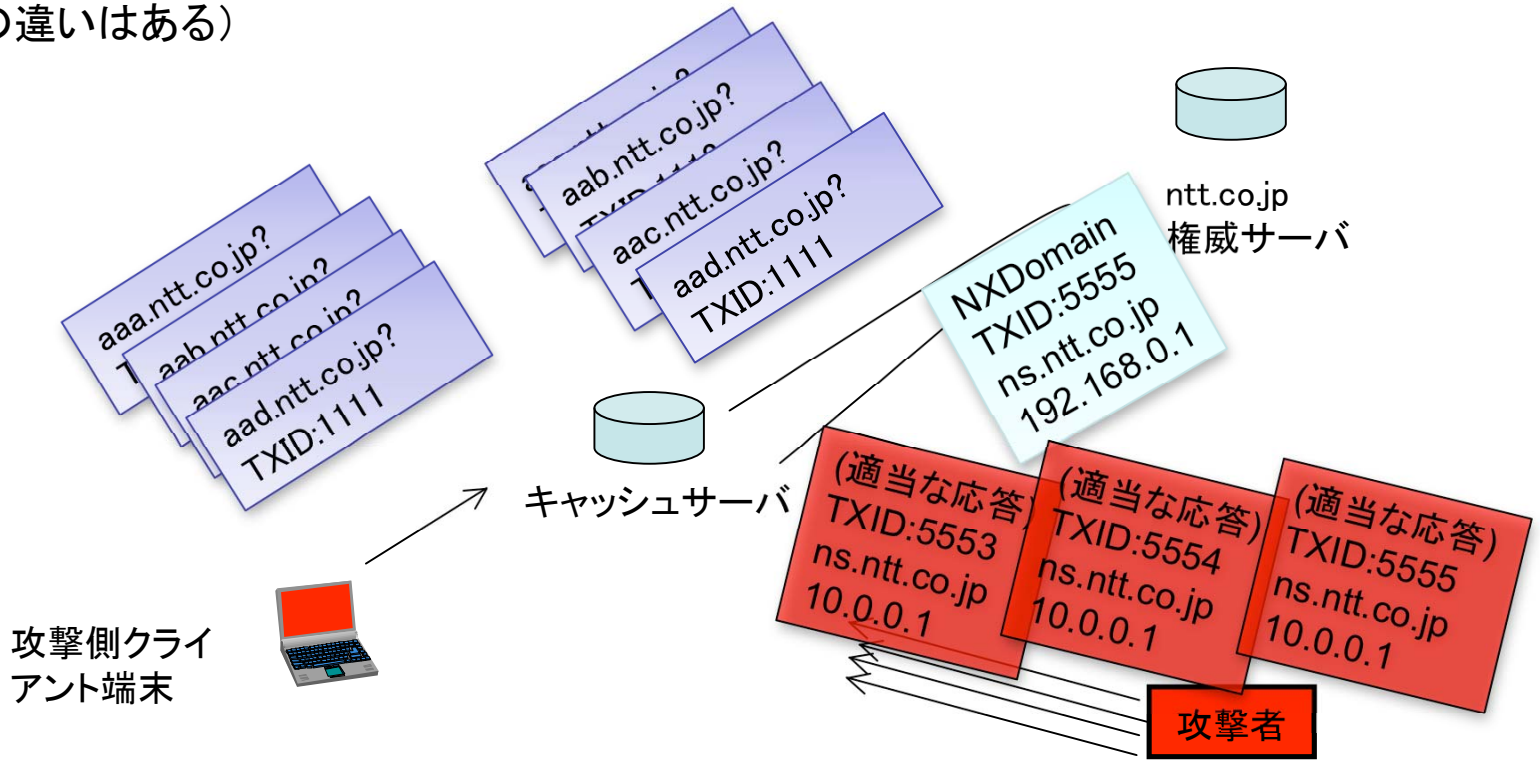
DNSキャッシュ汚染(2/3)

- DNSキャッシュ汚染攻撃自体は以前から知られていた攻撃.
- DNS問い合わせにおける基本的な応答認証
  - キャッシュサーバは権威サーバへの問い合わせにTXIDという16bitのIDを付与する.
  - 権威サーバからの応答のTXIDが問い合わせと同じであればその応答を信用する.
- 攻撃者が権威サーバより早くTXIDが一致する偽応答を返せば，キャッシュサーバはその偽応答を信用してしまう⇒TXIDのbrute force攻撃が可能
  - 問い合わせと応答のタイミングを合わせれば効率的な攻撃が可能
- キャッシュサーバは一定時間（TTL）応答をキャッシュする⇒TTLが長ければ，攻撃側クライアント端末が問い合わせを行っても権威サーバへの問い合わせは発生せず，攻撃回数は軽減される[民田]



DNSキャッシュ汚染(3/3)

- 今回(カミンスキー攻撃)は何が違うのか？
- 存在しないドメイン名を用いて毎回別のドメイン名を問い合わせる⇒TTLによる防御(攻撃確率の抑制)を無効化
- 問い合わせドメイン名自体でなく，応答に付随させる情報(別名，権威サーバ)で汚染．ただしこちらは以前からあり，権威外の情報は信用しないという対策がとられている
  ⇒今回は権威内の付随情報を利用する．
- 特定実装の脆弱性ではなく，プロトコル自体の脆弱性(実装によって攻撃パターンに対する脆弱性の違いはある)



経緯

- 2008年初め：IO Active社のセキュリティ研究者Dan KaminskyがDNSの脆弱性を発見
- 3月31日：関係者会議．対策スケジュールを決定．
- 7月8日：
  - 各CERTから DNSの脆弱性（Cache Poisoning攻撃)に関する Alertが発行
  - 8月6日に開催されるセキュリティ系会議（Black Hat 2008 USA)でDan Kaminskyが詳細手法を公開する旨を通達
  - パッチ対処に約一ヶ月間の猶予（のはずだった）
- 7月21日：脆弱性情報が流出
- 7月23日：攻撃コードが公開
- 7月29-30日：攻撃が開始
- 8月6日（当初予定通り）BlackHatでKaminskyが脆弱性の詳細について発表

被害実態

- AT&T
  - 2008/7/29にmetasploitブログにて報告．（脆弱性(非公式)公開の1週間後）
  - 汚染先：広告サイト

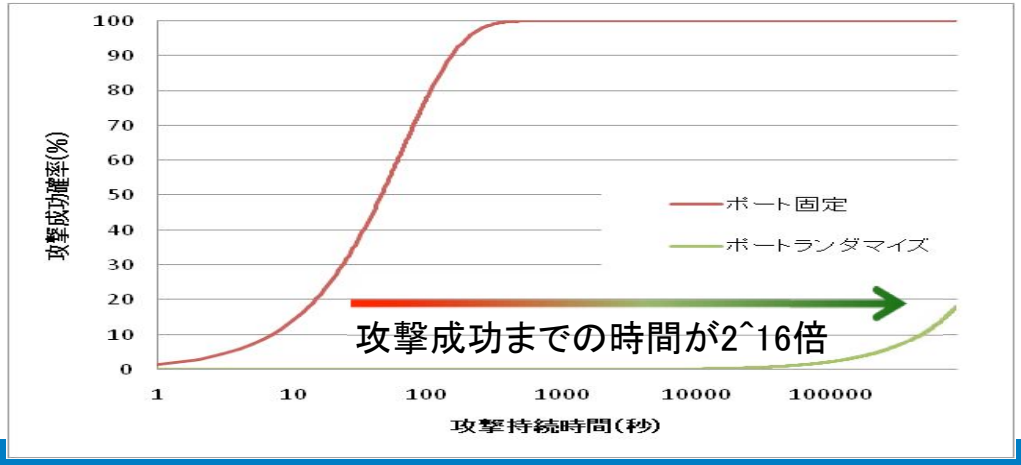
http://blog.metasploit.com/2008/07/on-dns-attacks-in-wild-and-journalistic.html

- 中国大手ISP
  - 2008/8/21にwebsense社ブログにて報告
  - 汚染先：マルウェアダウンロードサイト

http://securitylabs.websense.com/content/Alerts/3163.aspx

対策その1(ポート番号ランダム化)

- 送信ポート番号のランダム化
  - キャッシュサーバは送信ポート番号，TXIDの双方が一致した場合にのみ応答を信用する⇒TXIDに加えて送信ポート番号もランダマイズし，攻撃成功確率を低減させる(探索空間：2^16⇒2^32)
  - 2008/7/8に公開されたパッチが採った対策(一部のキャッシュサーバ実装は元々ランダマイズ機能あり)
- 単にパッチを当てるだけでは効果が無いケースあり．キャッシュサーバ上位のファイアウォール，ロードバランサで送信ポート番号を固定値に変更するケースがあり，設定チェックが必要．
  - 送信ポート番号ランダマイズによる性能劣化検証も必要．
- 攻撃成功確率は激減するが，パッチ対策済みサーバを10時間で汚染したという報告もあり(ただしほぼDoS攻撃)



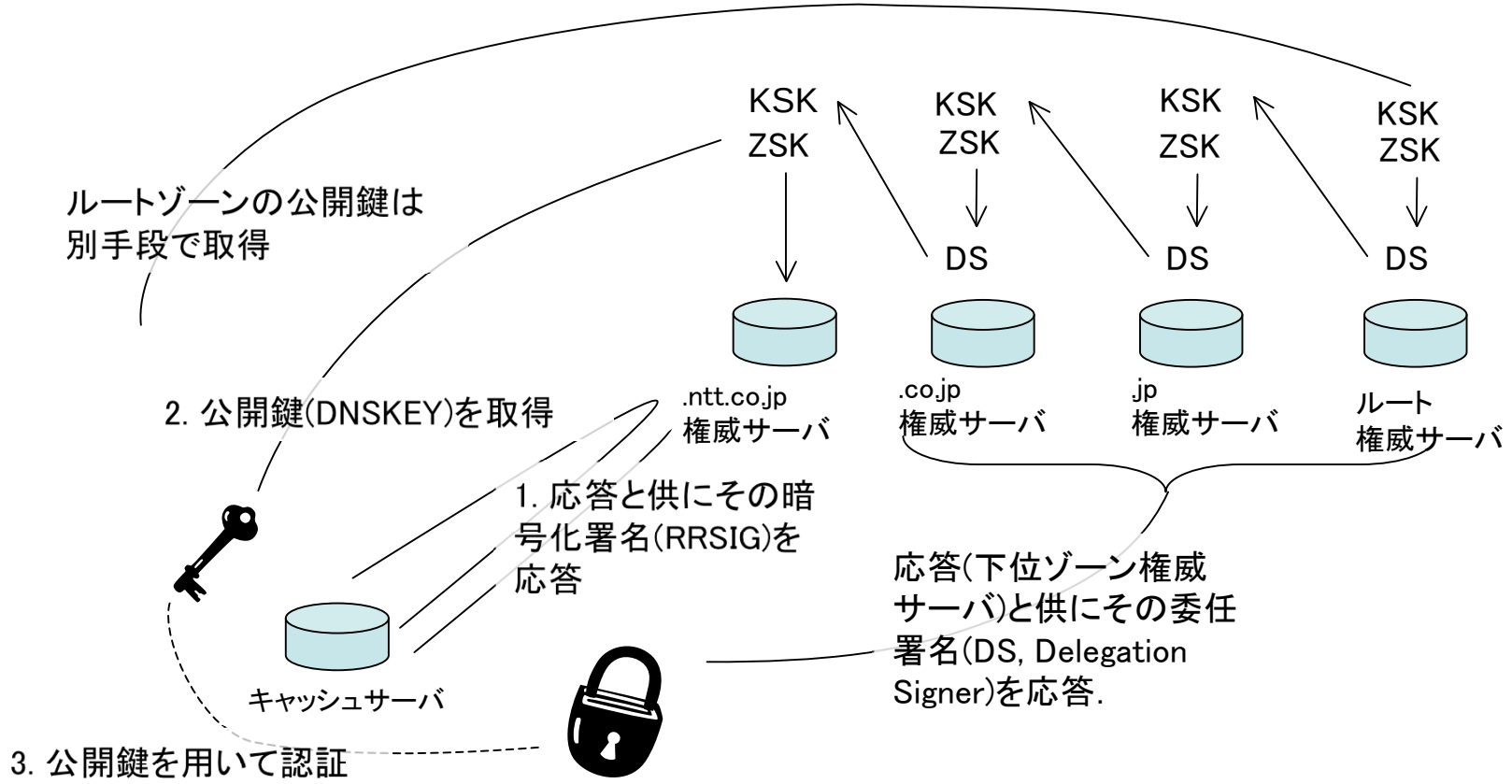
ポートランダム化未対応サーバ率

- 脆弱性公開前：7～8割⇒現在：2～3割
  - .com/.netへの問い合わせによる調査結果:20～22%[1]
  - .jpへの問い合わせによる調査結果:25%前後[2]
  - NetFlowデータを用いた調査結果：2割強[3]

1. Port and message ID analysis of resolvers querying .com/.net name servers (Matt Larson and Dave Blacka, Verisign)
2. Source port vulnerabilities in .JP (Izuru Shirai, JPRS)
3. Responsible Disclosure: A case study of CERT VU#800133, DNS Cache Poisoning Issue (Sid Faber, Cert/CC)

対策その2(DNSSEC)

- 抜本的対策
- 権威サーバが公開鍵暗号方式を用いて応答内容を電子署名
- 応答元ゾーン公開鍵の正当性をその上位ゾーンが承認(信頼の連鎖).



DNSSEC普及について

- ルートサーバから末端ゾーンの権威サーバ，およびキャッシュサーバが全て対応する必要あり(*)
  - 上記サーバ全てで費用対効果がマッチしているか？
  - キャッシュサーバ：サーバでのレスポンス処理の負荷増大
  - 権威サーバ：鍵管理等の運用コスト増大，トランザクション数，サイズの増大
  - *認証ツリーを別に作る手法もあり

- 現状
  - 導入Top Level Domain:スウェーデン，プエルトリコ，ブルガリア等．その他試験的導入は多数．.govは2008年末，.orgは2010年までに対応予定と表明．
  - DNSSEC普及調査結果[SecSpider]：12254ゾーン．ほとんどは試験的，もしくは.seドメイン
  - 試験的ゾーンを除く871ゾーンを調査[Eric08]．うち662ゾーンは上位からの信頼の連鎖無し．また連鎖による認証の失敗も多数．

[SecSpider] SecSpider: The DNSSEC Monitoring Project
[Eric08] Eric Osterweil, et.al, "Quantifying the operational status of the DNSSEC deployment," IMC '08.

対策その3(Workaround)

- キャッシュサーバでの対策
  - 外部からの問い合わせ遮断
    - ただし，botnetを用いる，WebにURIを仕込んでおく等，内部から問い合わせを発信させることは可能
  - 問い合わせレート制限
  - 偽装応答を検出したら，以後当該ドメイン名についてはTCPで問い合わせ

- その他提案中の技術
  - 0x20：権威サーバの問い合わせ時に大文字小文字を取り混ぜて問い合わせる（DNS的にはcase-insensiveなので問題ない）→ランダム性が増大．キャッシュサーバだけで対応が可能．
  - XQID：TXID 16bitに加えて24～63文字のプレフィックス(XQID)を問い合わせドメイン名に付与．→ランダム性が増大．権威サーバ，キャッシュサーバ双方の対応が必要．

対策その4(攻撃監視)

- 攻撃検出自体は比較的容易
  - 攻撃時には，クエリ無し応答が大量にキャッシュサーバに対して発生するため，それを検出すればよい
  - キャッシュサーバでの検出
    - BIND:クエリ無し応答ロギングパッチ
      - http://member.wide.ad.jp/~fujiwara/
    - Nominum: Vantio Detect and defend
  - 外部検出ツール
    - ISC SIE cache poisoning attempt detection tool
      - https://www.dns-oarc.net/node/141
    - NTT 情報流通プラットフォーム研究所
      - https://www.dns-oarc.net/files/workshop-2008/toyono.pdf

- いずれにせよモニタリングは重要